Pädagogische Hochschule Karlsruhe

Wissenschaftliche Hausarbeit

Thema: Geheimschriften in der Elementarstufe
unter besonderer Berücksichtigung des genetischen Prinzips

Fach: Mathematisch – naturwissenschaftlicher Fächerverbund

Verfasser: Sebastian Connette
Gottfried-Benn-Steige 1
66740 Saarlouis

Prüfer: Prof. Dr. Jochen Ziegenbalg
AR Thomas Borys

Arbeitszeitraum: 05.02.2009 bis 05.05.2009

Danksagung

Ich möchte mich an dieser Stelle bei einigen Personen bedanken, von denen jeder seinen ganz eigenen Beitrag zu dieser Arbeit geleistet hat.

Beginnen möchte ich meine Danksagung bei meinen beiden Betreuern Herrn Prof. Dr. Jochen Ziegenbalg und Herrn Thomas Borys, die mir stets mit Rat und Tat zur Seite standen. Das eine oder andere Gespräch enthielt nicht nur interessante Informationen, sondern auch Rechercheimpulse und einige hilfreiche Tipps für die praktische Umsetzung der Unterrichtseinheit die Gold wert waren.

Dann möchte ich mich herzlichst bei Frau Corinna Blume und der Klasse 4d bedanken, die mich immer wieder gerne zu sich einladen, um einige Stunden zu halten. Ich bekam die Chance die komplette, von mir geplante, Einheit in der Klasse durchzuführen und das obwohl sich Frau Blume und die Klasse dazu verpflichtet hatten sowohl eine Gruppe im Einführungspraktikum, als auch eine Blockpraktikantin aufzunehmen. Trotz der Zeitknappheit fand Frau Blume zwei Wochen für mich und stellte mir genügend Stunden zur Verfügung.

Als nächstes möchte ich meiner Freundin danken, die mich in Phasen purer Verzweiflung, in denen ich dachte die Decke stürzt über mir zusammen, stets beruhigte und die mich immer wieder aufs Neue motivierte mit neuem Elan an die Arbeit heranzugehen.

Ich möchte meinen Eltern danken, die mich seit meinem Studiengangwechsel vor einigen Jahren nur noch mehr unterstützen als sie dies ohnehin schon immer taten, da sie von meinem neuen Ziel, Lehrer zu werden, genauso überzeugt sind wie ich. Ihre Unterstützung bedeutet mir viel, da ich mich dank ihr voll und ganz auf mein Studium konzentrieren kann.

Schließlich möchte ich Frau Julia Trautz und Herrn Stefan Kuchenbrod danken, die ich zwar nie kennen gelernt habe, deren Hausarbeiten mir aber insbesondere in der Anfangszeit wichtige Hinweise darauf geliefert haben, wie man eine solche Arbeit sinnvoll angeht.

Vorwort

Als ich mir die ersten Gedanken zum Thema wissenschaftliche Hausarbeit machte, war mir bereits klar, dass die Arbeit eine Thematik behandeln muss, die mich selbst interessiert, die ich spannend finde, ja die sogar mein Gemüt bewegt. Ich wusste von Anfang an, dass nur ein solches Thema mir die nötige Motivation verschaffen würde mich über Monate hinweg Tag für Tag aufzuraffen, um mich damit auseinanderzusetzen und einige Sätze, oder manchmal auch Seiten, niederzuschreiben. Bevor ich mein Studium an der pädagogischen Hochschule Karlsruhe begann, studierte ich an der Universität Trier Rechtswissenschaften und schon damals spürte ich, wie ich mich insbesondere für Fälle ereiferte in denen die Privatsphäre einer Person verletzt war, denn ohne Privatsphäre kann es keine freie Meinungsbildung geben und meine persönliche freie Meinung ist mir wichtig. Dem Schutze der Privatsphäre können kryptographische Methoden dienen. Die Kryptographie interessiert mich aber auch noch aus einem anderen Aspekt. Ich finde es immer wieder erstaunlich wie vielfältig doch elementarste mathematische Methoden einzusetzen sind. Aus einer einfachen Additionsaufgabe der ersten Klasse in unserem Schulsystem wird so beispielsweise eine Buchstabenverschiebung die Nachrichten vor den Augen Unbefugter verschließt.

Allerdings würde meine eigene Motivation wohl kaum für eine wissenschaftliche Arbeit ausreichen, zu der auch noch eine Unterrichtseinheit gehört. Zu diesem Zweck sollte sie doch wenigstens einen Bereich tangieren, der für einen Großteil der Menschen und auch für unsere Schüler von Belang ist. Genau dazu fällt mir etwas ein, was bei mir in der Vergangenheit immer wieder zu Kopfschütteln führte.

Unsere Nachrichten zeichnen ein Bild dessen was uns interessiert, denn was nicht interessiert, das findet auch keine Zuschauer, Zuhörer oder Leser, mit anderen Worten: es liefert keine Quote und wird daher nicht gesendet oder geschrieben. Was immer gesendet wird sind Sensationsmeldungen: Unfälle, Kriege, Terroranschläge, Fluten und das, was unsere Politik auf solche Begebenheiten antwortet. Alle Jahre wieder kommt es nach Terroranschlägen oder Verbrechen zu Meldungen, dass die Politik die Maßnahmen zum Vorgehen gegen solche Terroristen und Verbrecher verschärfen will. Zu diesem Zweck werden dann Überwachungskameras aufgestellt, genetische Fingerabdrücke genommen, Telefone überwacht und ähnliches mehr und alle Jahre wieder folgt daraufhin der Aufschrei der Bevölkerung man stehe kurz vor

dem absoluten Überwachungsstaat. Immer wieder liest man von einem Alptraum der Massen, dem „gläsernen Bürger“. Schnell werden Demonstrationen gegen die neuen Maßnahmen eingeleitet. Der „gläserne Bürger“ oder besser gesagt das Verhalten, welches er bei den Menschen hervorruft, ist es, was mich den Kopf schütteln lässt. Ich glaube nicht, dass der „gläserne Bürger“ bevorsteht, ich glaube nicht, dass er irgendeine potentielle Zukunft darstellt, ich glaube vielmehr, dass der „gläserne Bürger“ schon seit langem die reale Gegenwart ist. Der Grund dafür liegt aber nicht bei Überwachungsmaßnahmen des Staates, er liegt vielmehr bei den Menschen selbst. Wie ich schon sagte, suche ich immer nach Themen die mein Gemüt bewegen und das tut die Vision des „gläsernen Bürgers“. Also kann ich es nur als riesengroßes Glück bezeichnen, dass es mir vergönnt war im Rahmen meines Lehramtsstudiums an der Pädagogischen Hochschule Karlsruhe einen Vortrag über die Überwachungsmethoden der Gegenwart zu halten und zumindest einigen Kommilitoninnen und Kommilitonen aufzuzeigen, wie nicht staatliche Überwachung zum „gläsernen Bürger“ führt, sondern der Mensch selbst. Die Gründe hierfür sind vielfältig, die häufigsten allerdings sind Unwissenheit, Naivität und Gleichgültigkeit. So ziehen wir beispielsweise in Demonstrationen gegen die Pläne der staatlichen Überwachung während wir gleichzeitig mit unseren Payback-Karten nicht nur Punkte sammeln, sondern auch umfassende Käuferprofile übermitteln. Was wir kaufen, wann und wo wir einkaufen gehen, welche Kreditkarten wir besitzen (inklusive sämtlicher Kreditkarteninformationen), etc. All diese Daten liefern wir den Betreibern der Payback-Karten. Spricht man die Leute darauf an, dann hört man meistens die gleichen Antworten „Das ist mir egal, ich bekomme dafür Rabatt.“ Man könnte es auch anders formulieren: „Wir verkaufen unsere Privatsphäre an große Firmen, Stückchen für Stückchen.“ Soviel zur Gleichgültigkeit. Die Unwissenheit spielt sich meistens in Bereichen ab, die wir kaum überblicken können. Der wahrscheinlich Bekannteste ist wohl das Internet. Das Internet wird von über einer Milliarde Menschen genutzt. Täglich werden mehrere Millionen E-Mails verschickt. Wer weiß da schon so genau, was abgefangen wird und was nicht, was gelesen wird und was nicht, kurz: „Was ist sicher und was nicht?“ Die knallharte Wahrheit muss lauten: „Wir wissen es nicht!“ Im schlimmsten Fall sogar ist gar nichts sicher und an dieser Stelle kommt die Naivität ins Spiel. Wir glauben einfach, das Internet sei sicher und wenn es das nicht ist, dann nehmen wir diese Unsicherheit eben billigend in Kauf, denn das Internet ist zumindest eines: gemütlich. 1999 wurde Scott McNealy (Chef von

Sun Microsystems) mit der Aussage berühmt „You have zero privacy anyway. – Get over it." Die Nachrichtenagentur heise online veröffentlichte am 24.10.2008 (also neun Jahre nach McNealys Aussage) einen Artikel, in dem sie schreibt, dass der Schutz der Privatsphäre in den kommenden zehn Jahren nicht besser werden wird. Die Auffassung der Experten sei, dass der Einzelne selbst für den Schutz seiner Privatsphäre sorgen muss.[1] Die Kryptographie bietet dafür reichlich Mittel, sie ist nämlich nicht, wie oftmals fälschlich angenommen, eine sehr junge Wissenschaft, die noch in den Kinderschuhen steckt, sondern eine traditionelle Wissenschaft, die bereits seit fast 4000 Jahren betrieben wird, nur stand sie in ihrer Geschichte meist nicht im Blickfeld der Öffentlichkeit, was wohl an der Sache selbst liegt, denn die Kryptographie ist nach wie vor am effektivsten, wenn keiner von ihr Notiz nimmt. Dennoch bleibt mir nichts anderes zu sagen, als dass die Kryptographie für uns heute wichtiger ist denn je. Während ich diese Zeilen tippe liegt neben mir eine Ausgabe der Süddeutschen Zeitung vom 28. / 29. März 2009. Auf der Titelseite prangt ein Foto von Hartmut Mehdorn und unter der Überschrift „Gewerkschaften: Mehdorn muss zurücktreten" steht als Untertitel zu lesen „Bahn ließ täglich 150.000 E-Mails ihrer Mitarbeiter kontrollieren [...]" Soviel noch einmal zur Sicherheit des Internets. Eigentlich ist es schon fast verwunderlich, dass Firmen wie die Bahn oder Lidl ihre Mitarbeiter überhaupt noch ausspionieren und sich nicht gleich die nötigen Informationen bei der Payback-Gesellschaft kaufen oder via Internet herunterladen. Vielleicht besteht ja doch noch ein Fünkchen Hoffnung, vielleicht liegt ja doch noch nicht alles im Argen. Solche Zeitungsmeldungen sind jedenfalls der beste Beweis dafür, dass wir uns um unsere Privatsphäre kümmern müssen.

Und gerade deshalb glaube ich, dass auch Kinder schon in frühen Jahren mit Kryptographie in Kontakt kommen sollten, dass wir unsere Schüler, wenn wir sie auf ihr Leben vorbereiten auch auf den Kampf um ihre Privatsphäre vorbereiten sollten, zumal sie in jungen Jahren ein großes Interesse an Geheimnissen haben und daher für solche Verfahren sehr gut zu motivieren sind. Dass die Auswahl der konkreten Inhalte dem Alter und Stand der Schülerinnen und Schüler anzupassen ist, sollte jedem klar sein, doch auch das einfachste Verfahren genügt bereits um ein gewisses Interesse zu schüren und die Kinder zur Beschäftigung mit dieser Thematik und Problematik anzureizen. Ich schreibe diese Arbeit also nicht nur für meine Prüfer, die Schülerinnen und Schüler die ich während meiner Unterrichtseinheit mit den

[1] http://www.heise.de/newsticker/Digitale-Zukunft-Keine-Chance-fuer-die-Privatsphaere--/meldung/117879.

kryptographischen Verfahren konfrontieren darf und mich selbst, sondern auch für alle (angehenden) Lehrerinnen und Lehrer, die sich Gedanken darüber machen, ob sie eine Einheit, oder sei es auch nur eine Stunde über Geheimschriften, Kryptographie, Steganografie, oder sonstige Geheimhaltungsmechanismen halten sollen oder nicht. Ich möchte euch allen eines sagen:

Tut es!

Tut es für euch, denn ihr werdet euch intensiv mit der Materie auseinandersetzen und sicherlich noch einiges lernen, was ihr selbst gebrauchen könnt.

Tut es für die Schüler, die eure Mühen hoffentlich aufnehmen und dadurch zukünftig vielleicht weniger naive und weniger gleichgültige Menschen im Umgang mit ihrer Privatsphäre sein werden, als wir das heute sind.

Tut es für deren Familien, die vielleicht von den Kindern, die ihr Wissen mit nach Hause tragen und es dort verbreiten, beeinflusst werden.

Tut es, denn es gibt nichts, wofür es sich mehr zu kämpfen lohnt, als für unser eigenes Leben und unsere Privatsphäre und jeder Mensch sollte die Möglichkeit bekommen diesen Kampf zu bestreiten.

Tut es!

Saarbrücken, den 30. März 2009

Sebastian Connette

Inhaltsverzeichnis

I. Geheimschriften in der Elementarstufe

1. Definition „Geheimschrift“

Das deutsche Universalwörterbuch aus dem Duden-Verlag weiß zu dem Begriff „Geheimschrift“ folgendes zu berichten:

> *„Geheimschrift, die: verschlüsselte oder unsichtbar gemachte Schrift, die nur für Eingeweihte entzifferbar sein soll: eine Geheimschrift entschlüsseln; in Geheimschrift schreiben.“*[2]

Dabei fallen die beiden Wörter „verschlüsseln“ und „entschlüsseln“ auf. Geheimschriften haben also offensichtlich etwas mit einem „Schlüssel“ zu tun.
Der Brockhaus schreibt:

> *„Geheimschrift, alle Arten der schriftlichen Darstellung geheimer Nachrichten, die für den Uneingeweihten nicht lesbar sind (z.B. verschlüsselte oder unsichtbar gemachte Nachrichten). Mit den Geheimschriften befasst sich die Kryptographie.“*[3]

Die Kryptographie ist also die Wissenschaft der Geheimschriften.

Im heutigen Internetzeitalter begibt sich eine Vielzahl der Menschen zu Recherchezwecken ins World Wide Web. Eine der bekanntesten Online-Enzyklopädien überhaupt ist Wikipedia. Das größte Problem dieses kostenfreien Enzyklopädie-Projektes ist, dass praktisch jeder Mensch von überall jeden Artikel bearbeiten kann; unabhängig von seinem tatsächlichen Wissensstand über das entsprechende Thema. Daher wird Wikipedia in der Wissenschaft oftmals gescholten und einen Blick in diese Enzyklopädie zu werfen gilt oftmals als unwissenschaftliches Vorgehen. Dass Wikipedia, trotz ihrer Problematik der freien Bearbeitung, manchmal besser ist als ihr Ruf, konnten Wissenschaftler des Magazins Nature aufzeigen. Wie das Online-Nachrichtenmagazin Heise-online berichtete, verglichen sie Wikipedia mit der renommierten Encyclopedia Britannica. Dabei schnitt Wikipedia nicht viel schlechter ab als die Encyclopedia Britannica.[4] Dieses Ergebnis darf natürlich nicht dazu verleiten sämtliche Recherchen ausschließlich über Wikipedia durchzuführen,

---

[2] Duden – Deutsches Universalwörterbuch.
[3] Brockhaus, die Enzyklopädie.
[4] http://www.heise.de/newsticker/Nature-Wikipedia-nahe-an-Encyclopaedia-Britannica--/meldung/67380, letzter Zugriff: 13.03.2009.

es zeigt aber wohl, dass nicht alles, was dort steht, immer sachlich falsch ist und man zumindest einen Blick in die Online-Enzyklopädie wagen darf.

Dieser Blick liefert auch sogleich ein sehr interessantes Ergebnis. Gibt man das Suchwort „Geheimschrift“ bei Wikipedia ein, so wird man direkt zum Begriff „Kryptographie“ weitergeleitet. Ein ähnliches Verhalten zeigt die Online-Enzyklopädie Encarta von der Firma Microsoft. Zwar gibt es hier keine direkte Weiterleitung, allerdings fördert ein Klick auf den Artikel mit der Überschrift „Geheimschrift“ ebenfalls die mit „Kryptographie“ überschriebene Seite zu Tage. Damit sehen beide Enzyklopädien diese beiden Begriffe offensichtlich als gleichbedeutend an. Die Encarta unterstreicht diese Gleichbehandlung indem sie der Herleitung des Wortes den Begriff „Geheimschrift“ selbst als Synonym hinten anstellt:

> „*Kryptographie (griechisch kryptein: verbergen; graphē: Schriftstück; Geheimschrift).*“[5]

Dabei handelt es sich offenbar tatsächlich um eine Schwäche der beiden Enzyklopädien, denn bereits die Brockhaus-Definition hat ja eine eindeutige Unterscheidung zwischen „Geheimschrift“ und „Kryptographie“ aufgezeigt, wenngleich beide Begriffe in einem engen Zusammenhang stehen.

Wenn wir uns nun in einem Bereich befinden, in dem es darum geht Informationen zu verschlüsseln oder geheim zu halten, dann fällt es uns nicht schwer zu sagen, dass diese Problematik keine rein deutsche ist. Wenn es sich allerdings um eine internationale Problematik handelt, dann lohnt es sich auch über die Grenzen der deutschen Sprache hinauszuschauen. Ein Blick ins Wörterbuch zeigt, dass das Wort „Geheimschrift“ im Englischen „cipher“[6] oder „cryptograph“[7] bedeutet. Dies führt zunächst zu einiger Verwirrung, da wir gerade erst die Begriffe „Geheimschrift“ und „Kryptographie“ voneinander abgegrenzt haben und der Wortlaut „cryptograph“, der nun „Geheimschrift“ bedeuten soll, sehr nahe am Wort „Kryptographie“ liegt. Doch diese Verwirrung lässt sich durch einen weiteren Blick ins Wörterbuch sehr schnell beheben, denn auch in der englischen Sprache wird zwischen „cryptograph“ und „cryptography“ (was schließlich Kryptographie bedeutet) unterschieden. Im

---

[5] MSN Encarta, http://de.encarta.msn.com/encyclopedia_761562343/Kryptographie.html, letzter Zugriff:13.03.2009.

[6] http://dict.leo.org/ende?lp=ende&lang=de&searchLoc=0&cmpType=relaxed&sectHdr=on&spellToler=on&chinese=both&pinyin=diacritic&search=geheimschrift&relink=on, letzter Zugriff: 13.03.2009.

[7] http://dict.leo.org/ende?lp=ende&lang=de&searchLoc=0&cmpType=relaxed&sectHdr=on&spellToler=on&chinese=both&pinyin=diacritic&search=geheimschrift&relink=on, letzter Zugriff: 13.03.2009.

englischsprachigen Raum weit verbreitet und bekannt ist die bereits weiter oben erwähnte Encyclopedia Britannica.

Die Encyclopedia Britannica erkennt den Begriff „cryptograph“ leider nicht und verweist dann auf ähnlich geschriebene Begriffe wie z.B. „cryptography“, was an diese Stelle nicht weiterhilft. Das Wort „cipher“ ist der Encyclopedia Britannica allerdings bekannt und wird folgendermaßen definiert:

„Any method of transforming a message to conceal its meaning.“[8]

Damit liefert die Encyclopedia Britannica eine weitere Definition, die den Begriff der „Geheimschrift“ noch etwas weiter fasst, als dies bislang Duden oder Brockhaus taten.

Über die Definitionen von Duden und Brockhaus hinaus lässt sich eine Geheimschrift nämlich nicht nur als die fertig verschlüsselte Information betrachten, sondern auch umfassender als irgendeine Methode zum Anfertigen solcher verschlüsselter Informationen. Eine solche Methode fiele in den Kanon der Verfahren zur Verschlüsselung von Informationen und damit in den Bereich der Wissenschaft, also der Kryptographie.

Ich persönlich favorisiere die „Geheimschrift“-Definition der Encyclopedia Britannica, da ich die der „verschlüsselten Nachricht“ als zu eng gefasst betrachte und unter „Geheimschrift“ auch die Methode und nicht nur das Ergebnis verstehe. Ich verwende diese Definition auch als Arbeitsdefinition. Wenn im Folgenden also von „Geheimschriften“ die Rede ist, so bezeichnet dies stets auch die Methode oder das Verfahren mit dem die verschlüsselte Botschaft hergestellt wurde.

Dass Online-Lexika tatsächlich nicht immer unkritisch zu Rate zu ziehen sind, möchte ich, dieses Thema abschließend, am Beispiel der Seite „Praxis-Lexikon, Wissen zum Anwenden“ aufzeigen. Praxis-Lexikon definiert den Begriff „Geheimschrift“ nämlich sehr treffend, absolut wahrheitsgemäß und mit einem gegen Null tendierenden Informationsgehalt, dafür aber hohem Unterhaltungswert mit den Worten:

„Die Geheimschrift ist eine Schrift, die geheim ist.“[9]

[8] The New Encyclopedia Britannica.
[9] http://www.praxis-lexikon.de/diy/diy-bauplan/g/geheimschrift.php, letzter Zugriff: 13.03.2009.

2. Geheimschriften im Schulunterricht

2.1. Primarstufe

2.1.1. Fachbereich Mathematik

2.1.1.1 Allgemein

Der Bildungsplan Baden-Württemberg[10] für die Grundschule beginnt den Abschnitt zum Fach Mathematik unter der Überschrift *„Zentrale Aufgaben des Mathematikunterrichts“* mit folgendem Satz:

> *„Aufgabe des Mathematikunterrichts aller Schuljahre ist es, Schülerinnen und Schüler für den mathematischen Gehalt alltäglicher Situationen und alltäglicher Phänomene sensibel zu machen und sie zum Problemlösen mit mathematischen Mitteln anzuleiten.“*[11]

Die Positionierung dieses Satzes lässt erschließen, dass es sich um die grundlegendste Aufgabe des schulischen Mathematikunterrichts handelt. Verstärkt wird diese Ansicht durch die klare Benennung des schulischen Zeitraums in dem diese Aufgabe erbracht werden soll, nämlich nicht innerhalb bestimmter Klassenstufen, sondern in „allen Schuljahren“. Geheimschriften in der Schule zu besprechen wäre demnach dann sinnvoll, wenn sie alltägliche Situationen und Phänomene darstellten. Dies wollen wir zunächst untersuchen.

Wenn wir von Geheimschriften sprechen, hat dies auch immer etwas mit Kommunikation zu tun. Eine interessante Definition von „Kommunikation“ hält der Internetauftritt der Bundeszentrale für politische Bildung bereit. Dort heißt es unter anderem:

> *„Kommunikation bezeichnet den Austausch von Informationen zwischen zwei oder mehreren Personen. Als elementare Notwendigkeit und wichtigstes soziales Bindemittel kann Kommunikation über Sprache, Mimik, Gestik, durch schriftlichen Austausch, Medien etc. stattfinden. …“*[12]

---

[10] Wenn im Folgenden nur noch von „Bildungsplan“ gesprochen wird, ist damit stets der Bildungsplan 2004 des Landes Baden-Württemberg gemeint.
[11] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 54.
[12] http://www.bpb.de/popup/popup_lemmata.html?guid=Q70R3S, letzter Zugriff: 14.03.2009.

Besonders im zweiten Satz wird die soziale Notwendigkeit von Kommunikation aufgegriffen. Kommunikation ist so wichtig für uns Menschen, dass auch ohne obige Definition jedem die Wichtigkeit der Kommunikation für unser soziales Leben klar gewesen wäre. Um diesem sozialen Gut nachkommen zu können, bedarf es mindestens zwei Personen, dem Absender und dem Empfänger. (Kommunikation kann auch zwischen Maschinen stattfinden. Diese Art der Kommunikation stellt aber keinen Aspekt dar, der von sozialer Bedeutung wäre.) Die Grundlage bildet zunächst der Absender. Er hat eine Information, die er einer anderen Person zukommen lassen möchte. Die Person des Empfängers nimmt also bereits in der Gedankenwelt des Absenders Gestalt an, noch bevor überhaupt eine Information verschickt wurde. Für den Absender sind dabei oftmals zwei Dinge wichtig. Zum einen, dass die Information überhaupt beim Empfänger ankommt, dass sie also nicht verloren geht und zum zweiten, dass kein anderer als der Empfänger die Information erhält. Auf beide Aspekte kann der Absender selbst achten, wenn er sich mit dem Empfänger trifft und ihm die Information persönlich zukommen lässt. Dies ist aber in unserer heutigen, globalisierten Gesellschaft oftmals nicht mehr möglich. Eine gewisse Faulheit der Menschen heutzutage trägt ihr Übriges dazu bei. Mobiltelefone beispielweise sind heute allgegenwärtig, doch neben dem Privileg dauerhafter Erreichbarkeit, werden sie immer wieder auch dazu missbraucht nur geringe Distanzen weniger Meter zu überbrücken. Doch gerade die Medien der Fernkommunikation, seien es nun Briefe, Telefone aller Art, SMS oder E-Mails weisen beträchtliche Sicherheitsrisiken auf. Einerseits muss eine Möglichkeit der Übertragung gefunden werden, damit der Absender sicher sein kann, dass seine Information auch den Empfänger erreicht. Andererseits bietet die Fernkommunikation sehr oft Möglichkeiten für potentielle Angreifer, für die die Information nicht bestimmt war, die aber in den Besitz der Information kommen möchten. Telefone können abgehört, Briefe, SMS oder E-Mails abgefangen und ausgelesen werden. Dem Umstand, dass die Privatsphäre des Menschen bezüglich der Informationen, die er auf dem Fernmeldeweg übermitteln möchte, zu schützen ist, hat unser Gesetzgeber im Grundgesetz Rechnung getragen. Dort heißt es in Artikel 10 I:

> *„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.“* [13]

[13] Art. 10 I GG.

Leider hält das Grundgesetz allein einen Angreifer noch nicht zwangsweise von seiner Tat ab. Diese Problematiken sind keine Entdeckungen der Neuzeit, aber wegen der weit verbreiteten technischen Mittel heutzutage ist es wichtiger denn je sich damit auseinanderzusetzen. Geheimschriften bieten für beide Problemgebiete unterschiedlichste Lösungen. So bilden sie mit ihren Aspekten der Codierung oft die Grundlage der technischen Übermittlung selbst und darüber hinaus sind sie geeignet Informationen so zu verschlüsseln, dass kein Angreifer sie lesen kann, selbst wenn er sie abfängt. In einer Zeit, in der Jobbewerber „gegoogelt" werden, um sich ein Profil des Bewerbers zu erstellen, bleibt nur jedem Menschen zu raten seine Geheimnisse auch wirklich geheim zu halten. Der Umgang mit dem Computer ist heutzutage für Schüler an der Tagesordnung und da das World Wide Web bekanntlich nichts vergisst, sollten sie schon heute an Geheimschriften herangeführt werden, wenn sie sich morgen für einen Arbeitsplatz bewerben möchten. Neben der Kommunikation finden sich Geheimschriften aber auch in vielen anderen alltäglichen Bereichen wieder, so zum Beispiel bei Online-Transaktionen, oder der Verwendung von Kreditkarten, aber auch in dem uns allen bekannten Strichcode EAN auf Produkten die wir einkaufen. Damit begleiten uns Geheimschriften also im Alltag, was uns wieder zu dem einleitenden Satz des Bildungsplanes zum Fach Mathematik zurückbringt:

> *„… für den mathematischen Gehalt alltäglicher Situationen und alltäglicher Phänomene sensibel zu machen …"*[14]

Eine Sensibilisierung muss in diesem Kontext nach obigen Ausführungen allerdings in zweifacher Hinsicht erfolgen. Zunächst einmal für die grundlegende Problematik, die schließlich dazu führt, dass Geheimschriften heute allgegenwärtig sind und dann im zweiten Schritt für den mathematischen Gehalt in den Geheimschriften und damit im Alltag. Die Geheimschriften selbst basieren zumeist auf mathematischen Grundoperationen, sodass der Gehalt deutlich erkennbar wird. Dies wird im Einzelfall im Rahmen dieser Arbeit an späterer Stelle noch einmal in den Fokus genommen.
Die beiden Sätze, die im Bildungsplan auf den von mir oben zitierten Satz folgen, zeigen den nächsten Schritt auf:

> *„Durch schulisches Lernen und Arbeiten erwerben die Kinder mathematisches Wissen und Können und lernen dieses zu nutzen. Es gelingt ihnen immer besser, allein und mit anderen, individuelle und*

[14] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 54.

gemeinsame Lösungswege und Antworten für Fragen und Probleme zu finden.“ [15]

Der Schüler soll also nicht bei der Erkenntnis des mathematischen Gehaltes einer alltäglichen Situation verharren, sondern diese Erkenntnis auch nutzen und zur Problemlösung verwenden. Insbesondere dafür bieten Geheimschriften vielfältige Möglichkeiten. Gerade die Anwendung muss bei einer Unterrichtseinheit über Geheimschriften im Mittelpunkt stehen. Eine Einheit, die sich nur damit begnügt den mathematischen Gehalt zu ermitteln ohne die Verfahren anzuwenden, ginge am Ziel vorbei.

Unter der nächsten Überschrift „Kompetenzen“ spricht der Bildungsplan von „mathematischem Grundwissen“:

„Im Mathematikunterricht erwerben die Schülerinnen und Schüler mathematisches Grundwissen, mathematische und übergreifende Kompetenzen.

Mathematisches Grundwissen beinhaltet unabdingbare Kenntnisse und Fertigkeiten. Dazu gehören solides Zahlenverständnis, das Beherrschen der Grundrechenarten, […]

Durch den zielgerichteten Umgang und durch die Anwendung des Grundwissens werden inhaltsbezogene Kenntnisse und Fertigkeiten zu mathematischen Kompetenzen weiterentwickelt.“[16]

Auch hier finden Geheimschriften erneut eine Berechtigung als Inhalt des mathematischen Unterrichts der Grundschule, da mit ihnen elementare Operationen, wie z.B. Addition und Subtraktion im Rahmen des Caesar-Verfahrens, geübt und vor allem praktisch angewandt werden können. Verfahren wie die Fleißner-Schablone bieten darüber hinaus Anreize zu geometrischen Überlegungen.

Und ganz nebenbei dient eine Einheit Geheimschriften auch dazu die Aspekte in den letzten beiden Abschnitten unter „Kompetenzen“ zu fördern:

„Beim Forschen und Fragen, beim Untersuchen und Entdecken, beim Ordnen, Vergleichen, Analysieren und Dokumentieren erwerben die Kinder elementare mathematisch-naturwissenschaftliche Kompetenzen. […]

[15] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 54.
[16] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 54.

Diese kreative Denk-, Lern- und Arbeitshaltung der Schülerinnen und Schüler aufzubauen und zu pflegen ist zugleich Ziel und Profil des Mathematikunterrichts in der Grundschule.“[17]

Im Folgenden verschaffen wir uns einen Überblick, über die von Geheimschriften tangierten Kompetenzen im Bildungsplan der Grundschule. Dabei folgen wir dem Aufbau des Bildungsplanes und schauen uns zunächst die Leitideen zu den Klassen 1 und 2 und anschließend die Leitideen der Klassen 3 und 4 an.

2.1.1.2. Kompetenzen Klasse 2

In der 1. Leitidee: „Zahl“ finden wir zunächst einen Bezugspunkt in den Grundrechenarten Addition und Subtraktion, die im Rahmen einiger Geheimschriften Anwendung finden und somit geübt werden können.
Im Rahmen der 3. Leitidee: „Raum und Ebene“ werden Vierecke behandelt, darunter auch der wohl bekannteste Vertreter dieser Gruppe, das Quadrat. Darüber hinaus fordert die Leitidee aber auch das eigene Herstellen symmetrischer Figuren und die Überprüfung solcher Figuren auf Symmetrie. Gerade der Aspekt der Symmetrie spielt eine große Rolle bei der Schablonenverschlüsselung nach Eduard Fleißner von Wostrowitz.
Die Wichtigkeit und zentrale Bedeutung von Geheimschriften haben mittlerweile wohl auch die Bildungsplaner erkannt und somit haben sie die Behandlung solcher Schriften konkret in den Bildungsplan mit aufgenommen. In Leitidee 4: „Muster und Strukturen“ steht wörtlich geschrieben:

„Die Schülerinnen und Schüler können

[…]

Zeichen- und Symbolkonstellationen als verschlüsselte Botschaften erkennen und diese nach einem Code entschlüsseln.“[18]

Und unter Inhalte werden dann nochmals „Geheimschriften“ und „verschlüsselte Botschaften“ genannt.
Die 5. und letzte Leitidee: „Daten und Sachsituationen“ beinhaltet schließlich das „Sammeln von Daten aus Experimenten, Texten und vereinfachten Darstellungen“[19].

[17] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 55.
[18] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 59.
[19] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 59.

Beispielhafte Inhalte sind diesbezüglich „Strichlisten“ und „Häufigkeitstabellen“. Diese Kompetenzen lassen sich im Rahmen des Brechens verschlüsselter Botschaften üben und einsetzen (doch auch dazu später mehr).

2.1.1.3 Kompetenzen Klasse 4

Die Kompetenzen, die die Schüler bis Ende der 4. Klasse erworben haben sollen, lesen sich ähnlich wie die bis Ende Klasse 2. Das ist im Sinne des Spiralprinzips nach Bruner auch nicht weiter verwunderlich.
Konkret bedeutet das zunächst, dass die 1. Leitidee erneut den Titel „Zahl“ trägt und auch hier finden sich wieder die Grundrechenarten Addition und Subtraktion. Zwar diesmal in schriftlicher Form und damit einen Schritt weiter (Spiralprinzip) als in den Klassen 1 und 2, aber die beiden Grundrechenarten spielen wieder eine Rolle und wie bereits oben erwähnt, tun sie das auch im Rahmen der Geheimschriften.
Die 3. Leitidee: „Raum und Ebene“ beinhaltet wieder den Punkt „symmetrische Figuren herstellen und Formen und Figuren auf Symmetrie überprüfen“.
In der 4. Leitidee: „Muster und Strukturen“ ist zwar diesmal nicht konkret von Geheimschriften die Rede, dennoch enthält sie einen Unterpunkt

> *„[…] Zeichen und Symbolkonstellationen als verschlüsselte Informationsquellen und als Notationsform in unterschiedlichen Zusammenhängen erkennen“.*[20]

Und auch in der 5. Leitidee: „Daten und Sachsituationen“ fordert der Bildungsplan das „Sammeln von Daten aus Beobachtungen, Experimenten, Texten und Darstellungen“ sowie das Ziehen von „Schlussfolgerungen“ daraus.

Zusammenfassend lässt sich also festhalten, dass Geheimschriften viele Aspekte der im Bildungsplan geforderten Kompetenzen ansprechen und das in allen vier Schuljahren. Darüber hinaus wird die Behandlung von Geheimschriften im Kompetenzbereich der Klasse 2 vom Bildungsplan sogar gefordert.

[20] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 61.

2.1.2. Fachbereich Deutsch

Da Geheimschriften im klassischen Sinne wegen ihrer mathematischen Grundlagen dem Fach Mathematik zugeordnet werden, soll die Analyse der Kompetenzen im Fach Deutsch nicht ganz so ausführlich erfolgen. Weil das Wort Geheimschrift aber den Wortteil „-schrift“ enthält, kann eine solche Analyse nicht gänzlich ausbleiben. Darüber hinaus rückt in den letzten Jahren immer häufiger der Begriff des fächerübergreifenden Unterrichts in den Fokus. Das ist zwar nichts Neues, es wird nur neu benannt, allerdings sollte auch diesem Umstand Rechnung getragen werden, zumal eine Verankerung der Geheimschriften in weiteren Fachbereichen und damit einer Fähigkeit der Abdeckung von Kompetenzen mehrerer Fächer gleichzeitig, der Geheimschrift als Unterrichtsthema nur zuträglich sein kann.
In Klasse 4 finden wir unter 1. „Sprechen“ z.B. den Punkt:

> *„Die Schülerinnen und Schüler können über das Gelingen von Kommunikation nachdenken und Konsequenzen daraus ziehen.“*[21]

Dazu gehört in erster Linie natürlich die direkte Kommunikation zwischen zwei oder mehreren Personen mit zeitlicher und örtlicher Nähe. Darüber hinaus kann Kommunikation aber auch, wie bereits weiter oben erwähnt, über eine zeitliche oder örtliche Distanz erfolgen. Dabei kommt es oftmals zu Problemen, die mit Hilfe von Geheimschriften gelöst werden können. Damit tragen Geheimschriften massiv zum Gelingen von Kommunikation bei.
Außerdem finden sich mit:

> *„Die Schülerinnen und Schüler können*
> *[…]*
> *mit Hilfe von handlungs- und produktionsorientierten Verfahren Texte untersuchen;*
> *[…]*
> *ästhetisch und kreativ mit verschiedenen Texten umgehen;*
> *[…]“*

im Rahmen des Punktes 2 „Lesen / Umgang mit Texten und Medien“ gleich zwei Aspekte auf die eine Einheit Geheimschriften Einfluss nimmt, denn ein Geheimtext wurde immer irgendwie produziert. Damit gehören das eigene Herstellen eines Geheimtextes und das Entschlüsseln mit Hilfe des entsprechenden Verfahrens

[21] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 50.

eindeutig auch in den ersten der beiden Punkte. Aber auch der zweite Punkt ist nicht zu unterschätzen. Der Verschlüsseln von Geheimschriften stellt zweifelsohne einen höchst kreativen Umgang mit dem ursprünglichen Klartext dar, darüber hinaus haben Geheimschriften auch eine gewisse Ästhetik und sei es nur die Ästhetik des Verfahrens und nicht des abschließend verschlüsselten Textes, doch das wird auch nicht gefordert, sondern ein ästhetischer Umgang mit dem Text.

Wenn man sich mit Geheimschriften auseinandersetzt, sticht einem bei der Lektüre des Bildungsplanes zum Fach Deutsch ein Punkt regelrecht ins Auge:

> *„Die Schülerinnen und Schüler kennen unterschiedliche Schrifttypen und Schriftzeichen aus unterschiedlichen Zeiten, Ländern und Kulturen (Erfindung des Buchdrucks).“*[22]

Hier wird zwar nicht direkt die Behandlung von Geheimschriften gefordert, allerdings führt uns dieser Wortlaut zu der Überlegung was eigentlich Schriftzeichen sind. Genau genommen sind Schriftzeichen nämlich nicht anderes als eine Codierung von Sprachlauten und damit befinden wir uns wieder beim Codierungsaspekt von Geheimschriften. Zwar würde heutzutage niemand die deutsche oder eine andere gebräuchliche Sprache konkret als eine Geheimschrift oder eine Geheimsprache bezeichnen, dass wir uns mit dem Codierungsaspekt der Sprache allerdings sehr nah an Geheimschriften befinden, zeigen spezielle Schriften wie z.B. der Braille-Code für Blinde. Außerdem steht dort ja gerade nicht, dass man Sprachen aus diesen Zeiten und Ländern lernen soll, das würde auch eher in den Bereich der Fremdsprachen gehören, sondern lediglich die Schriftzeichen, was uns unweigerlich an eine Methode von Julius Caesar erinnert, der einige seiner Texte zwar in lateinischer Sprache schrieb, allerdings mit griechischen Buchstaben.

Schließlich wäre da unter 4. „Sprachbewusstsein entwickeln“ noch der Punkt:

> *„Die Schülerinnen und Schüler können die Sprache, vor allem die Schriftsprache, zum Gegenstand ihres Nachdenkens machen;*
> *[…] “*[23]

und was wäre wohl besser dazu geeignet die Schüler zum Nachdenken über Schriften zu bewegen als Geheimschriften.

Wir finden also auch viele Anknüpfpunkte für Geheimschriften im Bildungsplan des Fachbereiches Deutsch.

---

[22] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 51.
[23] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 52.

2.1.3. Fachbereich Mensch, Natur und Kultur

Abschließend werfen wir auch noch einen Blick in den Bildungsplan des Fachbereiches Mensch, Natur und Kultur.
Hier werden wir zunächst in 3. „Kinder dieser Welt: sich informieren, sich verständigen, sich verstehen“ fündig:

„Die Schülerinnen und Schüler

[…]

entdecken Spuren verschiedener Kulturen in ihrer Alltagswelt.“[24]

Damit sind zwar in erster Linie Spuren von noch existierenden Kulturen gemeint, allerdings darüber hinaus auch Überbleibsel von früheren Kulturen, zu denen auch viele noch heute gebräuchliche Verfahren der Geheimschriften zählen. Spätestens in Klasse 4 steht dann aber konkret:

„Die Schülerinnen und Schüler können

[…]

Besonderheiten, Unterschiede und Gemeinsamkeiten von Kulturen aus Vergangenheit und Gegenwart erkennen;

[…]“[25]

und zu eben jenen Gemeinsamkeiten gehört auch die Notwendigkeit zur Verschlüsselung geheimer Informationen. Unterschiede bilden dann gegebenenfalls die unterschiedlichen Verfahren.
Unter 4. „Raum und Zeit erleben und gestalten“ fordert der Bildungsplan:

„Die Schülerinnen und Schüler können

[…]

Ereignisse und Erlebnisse als zeitlich gegliedert verstehen;

[…]“[26]

Dies kann auch eine in die zeitliche Abfolge gegliederte Einheit zu Geheimschriften leisten.
Die nächsten Punkte, die wir mit Geheimschriften bedienen können finden wir im Punkt 8. „Erfinderinnen, Erfinder, Künstlerinnen, Künstler, Komponistinnen und Komponisten entdecken, entwerfen und bauen, stellen dar“:

[24] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 101.
[25] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 105.
[26] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 101.

„Die Schülerinnen und Schüler

[…]

kennen Beispiele wichtiger technischer Erfindungen aus ihrem Alltag.“[27]

Auch Geheimschriften stellen wichtige technische Erfindungen dar, darüber hinaus bilden sie, wie bereits erwähnt, die Grundlage für viele weitere technische Mittel, die wir heute in unserem Alltag verwenden.

Außerdem steht unter der gleichen Überschrift weiterhin:

„Die Schülerinnen und Schüler können

[…]

einfache Gegenstände selbst herstellen und Werkzeuge sachgerecht benutzen;

[…]“[28]

Da viele Geheimschriften mit Hilfsmitteln arbeiten, bieten sie auch vielfältige Möglichkeiten solche Hilfsmittel herzustellen, z.B. die Caesar-Scheibe.

Geheimschriften bieten also eine ganze Menge an Ansatzpunkten die sie im Sinne des Bildungsplanes als Unterrichtsrelevant charakterisieren, sie werden sogar vom Bildungsplan als Unterrichtsinhalt gefordert. Darüber hinaus tragen sie mit ihrem hohen Grad an Interdisziplinarität zur Durchführung fächerübergreifenden Unterrichts bei.

2.2. Sekundarstufe I

Wenngleich der Schwerpunkt der vorliegenden Arbeit auf der Primarstufe liegt, so kann ein Blick darüber hinaus in die Anfangsklassen (Klassen 5 und 6) der weiterführenden Schulen nicht schaden.

2.2.1. Hauptschule

Bei der Betrachtung des Bildungsplanes für die Hauptschule fällt zunächst auf, dass Geheimschriften hier nicht konkret gefordert werden. Dennoch finden sich auch hier vielfache Anknüpfungspunkte die eine solche Unterrichtseinheit rechtfertig würden.

[27] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 103.
[28] Bildungsplan 2004 Baden-Württemberg Grundschule, S. 103.

So lässt sich auch hier noch einmal der Bezug zum Alltag hervorheben. Hinzu kommt:

> *„Das Fach Mathematik leistet dabei auch einen Beitrag zur Informationstechnischen Grundbildung.“*[29]

Wenn wir nun die Brücke zur Informationstechnischen Grundbildung schlagen, dann finden wir dort sehr schnell zu vermittelnde Aspekte die mit Gefahren zu tun haben, wie z.B.:

> *Klasse 6*
>
> *„Die Schülerinnen und Schüler können*
>
> *[…]*
>
> *die Gefahren bei der Preisgabe persönlicher Daten erkennen.“*
>
> *Klasse 9*
>
> *„Die Schülerinnen und Schüler können*
>
> *die grundlegenden Strukturen globaler Informationsnetze erkennen und Chancen und Risiken sowie die persönlichen und gesellschaftlichen Auswirkungen reflektieren;*
>
> *[…]*
>
> *mögliche Gefahren bei der ungeschützten Preisgabe persönlicher Daten im Internet erkennen und entsprechende Schutzmaßnahmen anwenden;*
>
> *[…]*
>
> *Die Schülerinnen und Schüler wissen um die Problematik der Sicherheit und Zuverlässigkeit und um Missbrauchsmöglichkeiten elektronisch gespeicherter Daten auch aus dem Internet und kennen entsprechende Schutzmaßnahmen.“*[30]

Auch hier fordern die Bildungsplaner nicht konkret Geheimschriften allerdings müssen wir uns die Frage stellen, wie vielfältig die Schutzmaßnahmen, welche die Schüler kennen sollen, überhaupt noch ausfallen können, wenn wir den wichtigen Wert der Kryptographie ausblenden.

[29] Bildungsplan 2004 Baden-Württemberg Hauptschule, S. 74.
[30] Bildungsplan 2004 Baden-Württemberg Hauptschule, S. 156.

2.2.2. Realschule

Auch im Bildungsplan für die Realschulen findet sich die Informationstechnische Grundbildung, allerdings fällt dem geneigten Leser zunächst im Abschnitt Mathematik eine interessante Formulierung auf:

> *„Mathematik ist eine Sprache, die Strukturen erfasst und darstellt. Sie bietet die Möglichkeit, Gegebenheiten der Realität zu beschreiben. Unerlässliche Grundlagen hierfür sind das Verständnis des Verhältnisses der Mathematik zur natürlichen Sprache sowie die Fähigkeit, formale und symbolische Sprache zu dekodieren und zu interpretieren.“*[31]

Hier findet zum ersten Mal der Codierungsaspekt der Sprache Erwähnung. Dass unsere Schrift eine Codierung unserer Sprachlaute ist und damit sehr nahe an der Verwendung von speziellen Codes liegt, hatte ich bereits weiter oben angeführt. Selbstverständlich beinhaltet darüber hinaus auch Sprache selbst einen Codierungsaspekt. Das erkennt man unter anderem daran, dass immer wieder neue Wörter in den Duden aufgenommen werden. Wir entwickeln nach wie vor neue Begriffe für Gegenstände, Situationen, Zustände, etc. um diese zu benennen. Dabei handelt es sich um nichts anderes als eine sprachliche Codierung solcher Begriffe.
Der Abschnitt zur Informationstechnischen Grundbildung beinhaltet darüber hinaus erneut die Besprechung der Gefahren und Risiken, sowie Gegenmaßnahmen dazu, die unser heutiges Kommunikationszeitalter birgt:

> *„Die Schülerinnen und Schüler können*
>
> *[…]*
>
> *mögliche Gefahren durch die ungeschützte Preisgabe persönlicher Daten sowie durch den Austausch von Dateien erkennen und Maßnahmen zum Schutz ergreifen(8);*
>
> *[…]“*[32]

Eine geeignete Maßnahme gegen die ungeschützte Preisgabe persönlicher Daten und den Dateiaustausch wäre offensichtlich die Daten gerade nicht ungeschützt, sondern geschützt weiterzugeben. Gleiches gilt für den Austausch von Dateien. Einen solchen Schutz bieten insbesondere kryptographische Verfahren.

[31] Bildungsplan 2004 Baden-Württemberg Realschule, S. 60.
[32] Bildungsplan 2004 Baden-Württemberg Realschule, S. 194.

2.2.3. Gymnasium

Die Hauptaufgabe des Mathematikunterrichts der Gymnasien unterscheidet sich nur wenig von der der übrigen Schulstufen:

> *„Zentrale Aufgabe von Schule ist es, den Schülerinnen und Schülern zu ermöglichen, ihre Rolle in der gegenwärtigen und zukünftigen Welt zu finden. Diese Aufgabe umfasst zwei wesentliche Bereiche. Einerseits muss Schule die Schülerinnen und Schüler befähigen, Phänomene ihrer unmittelbaren Lebenswelt zu verstehen und damit ihren Alltag aktiv gestalten zu können sowie geistige Orientierung und Urteilsfähigkeit zu entwickeln, die für eine aktive Teilnahme am kulturellen und demokratischen Leben einer Gesellschaft unerlässlich sind. Andererseits muss Schule langfristig auf eine spätere Berufsausübung beziehungsweise auf eine Berufsausbildung oder ein Studium vorbereiten.“*[33]

Grundsätzlich beschränkt sich dieser Abschnitt weder auf das Fach Mathematik, noch auf die Schulart Gymnasium. Hier wird der grundsätzliche Auftrag allgemein bildender Schulen beschrieben. Gerade das bietet uns aber einen Ansatzpunkt für Geheimschriften in allen Schulzweigen, denn wie bereits weiter oben erwähnt gehören Geheimschriften zu unserem Alltag, sie sind nicht mehr daraus wegzudenken und wenn das Verschlüsseln und Geheimhalten von Informationen für jeden einzelnen von uns bedeutsam ist, dann ist es das für kleinere und größere Firmen umso mehr. Eine Einführung in Geheimschriften scheint mir also gerade im Hinblick auf die Heranführung des Schülers an sein späteres Berufsleben unverzichtbar.

Selbstverständlich findet sich der Bereich Geheimschriften, wenn auch nicht wortwörtlich, auch in der Informationstechnischen Grundbildung wieder:

> *„Die Schülerinnen und Schüler wissen*
>
> *[…]*
>
> *um die Problematik der Sicherheit und Authentizität von Mitteilungen in globalen Netzen und kennen Möglichkeiten zur Wahrung der Persönlichkeitssphäre (8).“*[34]

[33] Bildungsplan 2004 Baden-Württemberg Gymnasium, S. 92.
[34] Bildungsplan 2004 Baden-Württemberg Gymnasium, S. 312.

Nichts anderes als die Verwendung kryptographischer Verfahren ist damit gemeint. Darüber hinaus beinhaltet der Bildungsplan für Gymnasien im Bereich Informationstechnische Grundbildung zum ersten Mal auch namentlich das Konzept der Codierung:

> *„Die Schülerinnen und Schüler kennen*
> *[…]*
> *grundlegende Ideen und Konzepte digitaler Informationsbearbeitung: Informationsbegriff, Kodierung (8), Ablaufsteuerung (10);*
> *[…]“*[35]

> *„Die Schülerinnen und Schüler können*
> *[…]*
> *grundlegende Ideen und Konzepte digitaler Informationsbearbeitung anwenden: Informationsbegriff, Kodierung, Ablaufsteuerung (10);*
> *[…]“*[36]

Damit geht die Behandlung kryptographischer Verfahren in den Gymnasien über den Aspekt der Geheimhaltung hinaus.

Die Betrachtung kryptographischer Konzepte drängt sich also in sämtlichen Schularten auf. Das ist auch aufgrund ihrer großen Relevanz für unser heutiges Leben nicht verwunderlich. Diesem Umstand muss zweifelsfrei Rechnung getragen werden.

2.3. Eigeninteresse der Schülerinnen und Schüler

Nachdem wir nun den vielfachen Bezug zu den unterschiedlichen Bildungsplänen gesehen haben, bleibt noch ein weiterer Punkt, der für die Behandlung von Geheimschriften spricht, offen: Das Motivationspotential dieser Thematik ist für Schüler enorm. Gerade in jungen Jahren bilden Geheimnisse aller Art einen regelrechten Anziehungspunkt für das Interesse der Kinder. Dieser Reiz und diese Spannung waren es auch, die in mir die Idee einer Arbeit über Geheimschriften in der Elementarstufe keimen ließen. Im Laufe meines Studiums absolvierte ich ein vierwöchiges Blockpraktikum in einer dritten Klasse. Eines Morgens kam eine

[35] Bildungsplan 2004 Baden-Württemberg Gymnasium, S. 313.
[36] Bildungsplan 2004 Baden-Württemberg Gymnasium, S. 313.

Schülerin auf mich zu und versuchte mir etwas mitzuteilen. Ich verstand kein Wort von dem was sie mir erzählte, denn sie verwandte eine Geheimsprache, die Löffelchensprache. Bei der Löffelchensprache wird hinter jedem Vokal eines Wortes ein „- lef -“ eingesetzt, sowie der Vokal selbst noch einmal wiederholt bevor es mit dem Rest des Wortes weitergeht.[37] Das Wort „Hallo“ klingt dann beispielsweise so: „Halefallolefo“. Dieser spielerische Umgang zeigte mir zum ersten Mal, dass junge Kinder bereits ein gewisses Grundinteresse für die Thematik des Geheimhaltens besitzen. Dass es sich um einen spielerischen Umgang handelte und das Interesse des wirklichen Verbergens noch nicht ganz so ausgeprägt war, zeigte einerseits die Mimik des Mädchens und zum anderen die Tatsache, dass diese Sprache sehr schnell in der gesamten Klasse verbreitet war, sodass ein wirkliches Geheimhalten gegenüber den Mitschülern nicht mehr möglich war. Dennoch glaube ich, nach dieser Situation, heute mehr denn je, dass Kinder ein hochgradiges Interesse an Geheimnissen haben. Wenn das aber bedeutet, dass die Behandlung von Geheimschriften nicht nur den Bildungsplan vielfältig tangiert, sondern auch noch in einem ausgeprägten Interesse der Schüler liegt, dürfen wir den Schülern dieses Thema nicht vorenthalten. Denn was kann es für einen Lehrer besseres geben, als ein Thema für das sich die Schüler engagieren und mit dem sie gleichzeitig auf die Probleme der heutigen Gesellschaft und damit ihrer Gegenwart und Zukunft vorbereitet werden?

[37] http://de.wikipedia.org/wiki/Spielsprache#L.C3.B6ffelchensprache, letzter Zugriff: 15.03.2009.

II. Das genetische Prinzip

1. Genese, Genesis

Eines der grundlegendsten Prinzipien der Mathematikdidaktik ist das genetische Prinzip. Dabei handelt es sich um ein Konzept zum Aufbau von Unterrichtseinheiten. Doch was bedeutet genetisch, bzw. genetischer Unterricht überhaupt?
Genetisch ist das Adjektiv zum Substantiv Genese. Die Begriffe „genetisch“ und „Genese“ sind griechischen Ursprungs. Sie kommen vom Wort „Genesis“ was soviel bedeutet wie „Geburt“, „Entstehung“ oder „Entwicklung“. Der eingedeutschte Begriff der Genese hat die gleiche Bedeutung.[38] „Genesis“ ist vielen Menschen aus der Bibel als die Bezeichnung des ersten Buches Mose bekannt, das mit der Schöpfungsgeschichte der Erde beginnt.
Ein genetischer Unterricht geht also von der Entstehung der Sache aus. Bevor ich nun allerdings tiefer in die Materie genetischen Unterrichts vordringe, möchte ich im Sinne dieses Prinzips zunächst auf einen Vorläufer zu sprechen kommen.

2. Die biogenetische Grundregel

2.1. Die Ontogenese rekapituliert die Phylogenese

1866 formulierte der deutsche Zoologe Ernst Haeckel nach Beobachtungen den Zusammenhang zwischen Ontogenese und Phylogenese in der biogenetischen Grundregel. Diese Regel besagt, dass die Ontogenese die Phylogenese rekapituliert.

2.2. Ontogenese

Das Wort Ontogenese setzt sich aus den griechischen Wortbestandteilen „on“ (= „Wesen) und „genese“ (wie bereits erwähnt „die Entstehung“) zusammen. Unter der Ontogenese versteht man die Entwicklung eines einzelnen Lebewesens oder Individuums.[39] Der Vorgang der Ontogenese reicht dabei von der befruchteten

[38] vgl. Duden – Deutsches Universalwörterbuch.
[39] vgl. http://de.wikipedia.org/wiki/Ontogenese, letzter Zugriff: 18.03.2009.
http://de.encarta.msn.com/encyclopedia_721544584/Ontogenese.html, letzter Zugriff: 18.03.2009.
http://www.britannica.com/EBchecked/topic/429382/ontogeny, letzter Zugriff: 18.03.2009.

Eizelle bis zum adulten Stadium und umfasst sämtliche Zwischenstadien, die in dieser Entwicklung durchlaufen wurden.

2.3. Phylogenese

Phylogenese setzt sich ebenfalls aus zwei griechischen Wortbestandteilen zusammen. „Phyle“ (= Stamm) und wiederum „genese“. In Abgrenzung zur Ontogenese bezeichnet die Phylogenese die historische Entwicklung der Gesamtheit, eines Stammes oder einer Gruppe bestimmter Lebewesen.[40]

Haeckels Regel besagt also, dass die Entwicklung des einzelnen Individuums in ihren Stadien dem Verlauf der Evolution der Gruppe von Lebewesen folgt, dem das Individuum angehört. Haeckel bezieht sich dabei auf Beobachtungen und Forschungen des deutschen Embryologen Karl Ernst von Baer, der bereits 1828 erkannte, dass sich die Embryonen nahe verwandter Spezies deutlich weniger unterscheiden, als die jeweiligen adulten Formen.[41]

2.4. Kritik an der biogenetischen Grundregel

Wenn ich hier von Kritik spreche, so möchte ich zunächst festhalten, dass ich mich auf die wissenschaftliche Kritik an Haeckels biogenetischer Grundregel beschränke und nicht auf die Streitigkeiten zwischen Haeckel und den Kreationisten oder sonstiger Gegner der Evolutionstheorie eingehen möchte.
Haeckel wurde zunächst vorgeworfen, dass Ontogenese, in seinem Verständnis, gleichzusetzen wäre mit Embryonal- oder Individualentwicklung und dabei Aspekte der Botanik, namentlich der Generationswechsel bei Pflanzen, gänzlich ausgeblendet würde.[42] Außerdem glauben viele Wissenschaftler, dass Haeckel seine Skizzen gefälscht habe, um seiner Regel eine Grundlage zu verschaffen. Dazu führen Historiker allerdings an, dass Haeckels Zeichnungen die Wahrnehmung am

[40] vgl. http://de.wikipedia.org/wiki/Phylogenese, letzter Zugriff: 18.03.2009.
http://de.encarta.msn.com/encyclopedia_721544795/Phylogenese.html, letzter Zugriff: 18.03.2009.
http://www.britannica.com/EBchecked/topic/458573/phylogeny, letzter Zugriff: 18.03.2009.
[41] vgl. http://de.wikipedia.org/wiki/Baersche_Regel, letzter Zugriff: 18.03.3009.
[42] vgl. http://de.wikipedia.org/wiki/Biogenetische_Grundregel#Wissenschaftliche_Kritik, letzter Zugriff: 18.03.2009.

Anfang des 19. Jahrhunderts widerspiegeln würden, da er diese oftmals von seinen Vorgängern übernahm.[43]

2.5. Die biogenetische Grundregel heute

Fakt ist, dass die Wissenschaft Haeckels These heute als „nicht mehr haltbar" tituliert, sodass sie den Status als „Gesetz" verloren hat und sich daher heute nur noch als Regel bezeichnen darf. Dennoch kommt es auch heutzutage immer wieder zu Entwicklungen die Parallelen zu der von Haeckel aufgestellten Regel aufzeigen, sodass sie nicht gänzlich in Vergessenheit geraten ist.
Während der Versuch die Rekapitulationstheorie auf die Bereiche der Entwicklungs- und Evolutionspsychologie anzuwenden lange als verfehlt galt, weist Stephen Mithen auf Parallelen zwischen der kognitiven Entwicklung der Menschheit und der des Kindes hin.[44] Während Gerhard Medicus in seinem Aufsatz „The Inapplicability of the Biogenetic Rule to Behavioral Development" aufzeigt, dass Haeckels These keine Relevanz für die Verhaltensentwicklung hat und dies auch begründet[45], weist Irenäus Eibl-Eibesfeldt in seinem Werk „Grundriss der vergleichenden Verhaltensforschung" darauf hin, dass Wahrnehmung und Handeln des Menschen doch stammesgeschichtlich bestimmt sind.[46]

3. Das genetische Prinzip

Neben dieser Kontroverse entwickelt sich in der Pädagogik die „genetische Methode". Nach Martin Wagenschein ist das genetische Prinzip dreigliedrig. Es unterteilt sich in das genetische Prinzip, das auch das Wichtigste und damit namensgebende ist, das sokratische Prinzip und das exemplarische Prinzip.[47] Die sokratische Methode befindet Wagenschein als wesentlich, da sich, seiner Meinung nach, das „Erwachen geistiger Kräfte am wirksamsten im Gespräch vollzieht".[48] Er

[43] vgl. http://de.wikipedia.org/wiki/Biogenetische_Grundregel#Wissenschaftliche_Kritik, letzter Zugriff: 18.03.2009.
[44] vgl. http://de.wikipedia.org/wiki/Biogenetische_Grundregel#Wissenschaftliche_Kritik, letzter Zugriff: 13.03.2009.
mit Verweis auf Mithen, Stephen: the prehistory of the mind, 2003, 66-68.
[45] http://homepage.uibk.ac.at/~c720126/humanethologie/ws/medicus/block6/HumanDevelopment.pdf, letzter Zugriff: 18.03.2009.
[46] vgl. dazu auch http://erl.orn.mpg.de/~fshuman/de/hpeibl.html, letzter Zugriff: 18.03.2009.
[47] Wagenschein, Martin: Verstehen lehren, S. 75.
[48] Wagenschein, Martin: Verstehen lehren, S. 75.

führt an, dass ein solcher Unterricht aufgrund der Gründlichkeit nur exemplarisch sein kann, dies aber auch sein darf.[49] Das genetische Prinzip geht, wie bereits weiter oben erwähnt, von der Sache aus. Es geht darum dem Lernenden einen sehr viel tieferen Einblick in die Materie zu gewähren, indem er sich mit der ursprünglichen Problematik auseinandersetzt und probiert die Lösung selbst zu finden und dadurch schließlich neben der Lösung auch den Weg, sowie Sinn und Zweck, also das „warum" erkennt. Wagenschein schreibt dazu:

> *„Nur ist die Entdeckung des Systems (besser: der Systemisierbarkeit eines Gegenstandsbereiches) psychologisch und pädagogisch gesehen, etwas ganz anderes als die Kenntnisnahme (auch die verstehende), der dem Fachmann vorliegenden (nicht dem Anfänger) fertigen Strukturen: mit Hilfe von Denkwerkzeugen, die zu diesem Zweck (dem Schüler nicht erkennbaren Zweck) vorher eingeübt werden."*[50]

Es war Felix Klein, der sich im Rahmen des genetischen Prinzips konkret auf die biogenetische Grundregel Haeckels berief.[51] Gegen das Heranziehen von Haeckels Theorie ist einzuwenden, dass es nicht sinnvoll sein kann das lernende Individuum alle Fehlschläge und Wirren der geschichtlichen Entwicklung nachmachen zu lassen. Doch der Grundtenor seiner Aussage sollte nicht verkannt werden. Dieser ist nämlich nach Klein, den Menschen zum wissenschaftlichen Denken hinzuführen.[52]

Wittenberg erkannte die Kontroverse um Kleins Berufung auf die biogenetische Regel Haeckels und relativierte daher die gesamte Rekapitulation im genetischen Unterricht wie folgt, indem er den Punkt der Wiederholung sämtlicher historischer Fehler ausklammert und noch einmal auf den wesentlichen Kern des genetischen Prinzips aufmerksam macht, nämlich die Mathematik neu zu erleben und nachzuvollziehen.[53] Auch Otto Toeplitz verfolgt diese Auffassung wenn er schreibt, dass er aus der Geschichte nur „die Motive für die Dinge herausgreifen will" und noch einmal betont, dass es nicht „um die Geschichte geht, sondern um die Genesis der Probleme, der Tatsachen und Beweise".[54]

Nach Wittenberg ist das genetische Prinzip mindestens immer dann anzuwenden, wenn der fertige Gegenstand aufgrund von Komplexität nicht vermittelt werden kann,

---

[49] Wagenschein, Martin: Verstehen lehren, S. 75.
[50] Wagenschein, Martin: Verstehen lehren, S. 79.
[51] Vgl. Wittmann, Erich: Grundfragen des Mathematikunterrichts, S. 132.
[52] Wittmann, Erich: Grundfragen des Mathematikunterrichts, S. 133.
[53] Wittenberg, Alexander Israel: Bildung und Mathematik, S. 59.
[54] Toeplitz, Otto, zitiert in: Wittmann, Erich: Grundfragen des Mathematikunterrichts, S. 134.

denn es erscheint ihm sinnfrei, eine Sache zu unterrichten, die das Individuum nicht verstehen kann. An diese Stelle soll dann die Rekapitulation treten, um dem Schüler klarzumachen, wieso er so rechnen kann, wie er das tut. In diesem Sinne bezeichnet Wittenberg das genetische Prinzip nicht als einen Grundsatz historischer Treue, sondern einen der Sachgemäßheit, der zur Wissenschaft gehört.[55]

Toeplitz weist darüber hinaus auf das „lebendig werden" historischer Forschungen, sowie Spannung und Aufregung eines solchen historischen Suchvorganges hin (am Beispiel der Infinitesimalrechnung).

> *„[…] alle diese Gegenstände der Infinitesimalrechnung, die heute als kanonisierte Requisiten gelehrt werden, […], und bei denen nirgends die Frage berührt wird: warum so? wie kommt man zu ihnen?, alle diese Requisiten also müssen doch einmal Objekte eines spannenden Suchens, einer aufregenden Handlung gewesen sein, nämlich damals, als sie geschaffen wurden. Wenn man an diese Wurzeln der Begriffe zurückginge, würden der Staub der Zeiten, die Schrammen langer Abnutzung von ihnen abfallen, und sie würden wieder als lebensvolle Wesen vor uns entstehen."*[56]

Der Staub und die Abnutzungserscheinung sind dabei keine natürliche Erscheinung, sondern das Ergebnis einer Didaktik, die das Beschreiten eines solchen Weges vermeidet und nur das fertige Ergebnis präsentiert.[57] Es sei außerdem nicht zu vergessen, dass eine solche Spannung und Dramaturgie ein sehr großes Motivationspotential bieten können. Des Weiteren kann es in einer gewissen Befriedigung oder Genugtuung enden, wenn der Weg der Neuerschließung bis zum Ende des Problems gelungen ist, insofern macht Unterricht dann auch Freude.

Das genetische Prinzip gehört heute zu den elementarsten Prinzipien des Unterrichtens, insbesondere in wissenschaftlichen Bereichen, wie der Mathematik oder den Naturwissenschaften. Ihre Wichtigkeit erkannte auch der Reformpädagoge John Dewey. Er bezeichnete das genetische Prinzip als den vielleicht größten wissenschaftlichen Fortschritt der zweiten Hälfte des 19. Jahrhunderts.[58]

---

[55] Wittenberg, Alexander Israel: Bildung und Mathematik, S. 146.
[56] Toeplitz, Otto, zitiert in: Wittmann, Erich: Grundfragen des Mathematikunterrichts, S. 133.
[57] Wagenschein, Martin: Verstehen lehren, S. 102 f.
[58] Dewey, John: Demokratie und Erziehung, S. 283 f.

Zu den bekanntesten Persönlichkeiten, die sich mit der genetischen Methode beschäftigt haben, zählt zweifelsfrei Jean Piaget. Piaget war Schweizer Entwicklungspsychologe und hat in seinen Forschungen die Bedingungen aufgezeigt, die zur Entwicklung von Wissen, sowohl in der Wissenschaft, als auch im Individuum führen.[59] Dabei kam er zu dem Ergebnis, dass diese Bedingungen weitgehend die gleichen sind. Aus diesen Ergebnissen heraus entwickelte Piaget ein Stufenmodell zur kognitiven Entwicklung von Kindern. Dabei unterscheidet er vier Entwicklungsstufen:

1. Sensomotorisches Stadium
2. Präoperationales Stadium
3. Konkretoperationales Stadium
4. Formaloperationales Stadium[60]

Piagets Modell zählt im mathematischen Bereich zu den grundlegenden Modellen der Fachdidaktik. Mit diesem Wissen kann es einerseits nicht verwundern, dass es bereits in der Fachdidaktik im ersten Semester des mathematischen Studiums an der Pädagogischen Hochschule Karlsruhe gelehrt wird. Andererseits lässt die Tatsache, dass dieses Modell im ersten Semester gelehrt wird, für den Laien aber auch wieder Rückschlüsse auf dessen Bedeutung in der mathematischen Fachdidaktik zu.

Ich möchte das Kapitel zum genetischen Prinzip mit einem Zitat von Martin Wagenschein beenden:

> *„Nach diesen (begrifflichen) Zwischenbemerkungen möchte ich nun am Genetischen Lehren noch eines besonders loben: es schützt uns vor unserer häufigsten Versuchung (entschuldbar durch Stofffülle und hohe Klassenfrequenz): Abstraktionen zu verfrühen.“*[61]

[59] Wittman, Erich: Grundfragen des Mathematikunterrichts, S. 59.
[60] de.wikipedia.org/wiki/Jean_Piaget#Theorie_.C3.BCber_die_Entstehung_von_Identit.C3.A4t, letzter Zugriff: 18.03.2009.
[61] Wagenschein, Martin: Verstehen lehren, S. 98.

III. Das Codieren von Nachrichten

1. Nachrichtenübertragung

Die Übertragung einer Nachricht bedarf stets dreier grundlegender Dinge:

- Einen Absender der Nachricht

- Einen Empfänger der Nachricht

- Und einen Nachrichtenkanal.

Abbildung 3.1

Der Nachrichtenkanal kann jedoch niemals ohne eine Codierung überwunden werden. Diese Codierung geschieht praktisch automatisch. Wenn wir sprechen, dann Codieren wir unsere Nachricht mit Lauten die der Empfänger verstehen kann. Genau das ist eine Codierung. Eine Codierung ist nämlich nichts weiter als eine bestimmte Vorschrift zur Umwandlung der Nachricht in einer Form, die für den Empfänger verständlich ist.[62] Der Codierungsaspekt von Sprache wird besonders deutlich bei der Unterhaltung mit Menschen, die eine andere Sprache sprechen. Die Kommunikation über zwei unterschiedliche Codierungen funktioniert nicht. So gesehen ist aber nicht nur unsere Sprache eine Codierung, sondern auch unsere Schrift, Telefonate, E-Mails, SMS, usw. Codierungen treten überall dort auf, wo kommuniziert wird und ohne diese Codes wäre die Kommunikation nicht möglich.

[62] http://de.wikipedia.org/wiki/Code, letzter Zugriff: 23.04.2009.

2. Codierungsarten[63]

Im Verlauf der Menschheitsgeschichte wurden Entwicklungen und Fortschritte gemacht, die ganz neue Formen der Codierung bedurften, man denke beispielsweise an die Telegrafie. Neue auftretende Probleme mussten gelöst werden, daher gibt es heute eine unglaubliche Menge an Codes für ganz unterschiedliche Zwecke, wenngleich alle Codes nach wie vor der Kommunikation dienen. Probleme beim Empfänger, weil er beispielsweise sehgeschädigt ist und keine geschriebenen Nachrichten lesen kann, führten beispielsweise zur Entwicklung des Braille-Codes. Eine ganze Flut an neuartigen Codierungen brachte der aufstrebende Computer mit sich. Daten mussten im Computer gespeichert werden. Die Standardisierung von Zeichen führte zum ASCII und Unicode. Das World Wide Web verbindet über eine Milliarde Menschen miteinander. Es wird in vielerlei Hinsicht zur Kommunikation genutzt. Sei es in so genannten Chatrooms, per E-Mails oder auch zum Austausch von Datenpaketen. Doch die Kapazitäten der Datenleitungen sind beschränkt. Um diese Kapazität nicht zu sprengen, wurden Codes zur Komprimierung entwickelt (z.B. Huffman-Code). Diese unüberschaubare Datenflut führt leider mitunter dazu, dass Informationen oftmals unbedacht kopiert werden und die Quelle sich irgendwann nicht mehr feststellen lässt. In der Folge entstanden Identifikationscodes, wie etwa digitale Wasserzeichen. Und schließlich gibt es dann noch das uralte Problem, dass sich Angreifer unbefugt Kenntnis über Nachrichten verschaffen, indem sie diese abfangen und auslesen. Auch für diese Problematik gibt es Codes. Mit solchen Codes beschäftigen sich Geheimschriften, bzw. die Kryptologie. Da diese Art von Codes der Schwerpunkt dieser Arbeit sind, werden sie im nächsten Teil behandelt. Anschließend möchte ich noch einige andere ausgewählte Codes erläutern.

[63] Ziegenbalg, Jochen: Codierung und Kryptographie, S. 2.

IV. Kryptologie

1. Definition

Zu Beginn dieser Arbeit habe ich mich mit dem Begriff der „Geheimschrift“ auseinandergesetzt und dabei eine Definition des Brockhaus herangezogen, die einen Zusammenhang zwischen den Begriffen „Geheimschrift“ und „Kryptographie“ aufzeigte. Dort hieß es:

> *„Mit den Geheimschriften befasst sich die Kryptographie.“*[64]

Dagegen ist grundsätzlich nichts einzuwenden, allerdings ist die Kryptographie nur ein Teil eines umfassenderen Gebietes, der Kryptologie. Kryptologie setzt sich zusammen aus den griechischen Wörtern „kryptos“ (= geheim) und „logos“ (= das Wort).[65] Die Kryptologie beschäftigt sich also mit der Geheimhaltung von Informationen. Das allein grenzt sie aber noch nicht von der Kryptographie ab und daher kommt es auch in der Wissenschaft immer wieder vor, dass Kryptologie und Kryptographie weitgehend synonym verwandt werden:

> *„Manche Leute unterscheiden zwischen Kryptographie, […], Kryptoanalyse, […] und bezeichnen mit Kryptologie die Gesamtheit dieser Wissenschaften. Es besteht aber keine Gefahr von Missverständnissen, wenn man Kryptographie und Kryptologie synonym benutzt.“*[66]

Während Beutelspacher die unterschiedlichen Ansichten dennoch darstellt, fällt dies bei anderen Autoren manchmal komplett weg:

> *„Die Kryptologie, die Lehre von den Geheimschriften, […]“*[67]

Vergleicht man diese kurze Darstellung mit der Geheimschrift-Definition des Brockhaus, so stellt man tatsächlich fest, dass eine Unterscheidung in Kryptologie und Kryptographie häufig nicht vorgenommen wird.

Ich muss Herrn Beutelspacher aber dahingehend widersprechen, wenn er anführt, dass es sich bei denjenigen, die zwischen Kryptographie und Kryptoanalyse unterscheiden, nur um „manche Leute“ handelt. Diese Unterscheidung wird von den Autoren im überwiegenden Teil der mir zur Verfügung stehenden Quellen durchgeführt:

---

[64] Brockhaus, die Enzyklopädie.
[65] http://www.britannica.com/EBchecked/topic/145058/cryptology, letzter Zugriff: 20.03.2009.
[66] Beutelspacher, Albrecht: Kryptologie, S.2.
[67] Wobst, Reinhard: Abenteuer Kryptologie, S.11.

„Kryptologie vereinigt Kryptographie und Kryptanalyse.“[68]

„Der Zweig der Mathematik, der Kryptographie sowie Kryptoanalyse umfasst, ist die Kryptologie.“[69]

Und auch Friedrich Bauer unterscheidet diese Begriffe wenn er schreibt:

„[…] die Kryptologie, die Lehre von den Geheimschriften und ihrer unbefugten Entzifferung, […]“[70]

Auch die lexikalischen Werke sehen die „Kryptologie“ als Oberbegriff:

„Kryptologie, Wissenschaft von der Ver- und Entschlüsselung von Sprachzeichen bzw. dem Ver- und Entschlüsseln von Geheimsprachen.

[…] Sie besteht aus zwei Teilwissenschaften, der Kryptographie und der Kryptoanalyse.“[71]

„Die Kryptologie lässt sich in die beiden Gebiete Kryptographie und Kryptoanalyse unterteilen.“[72]

„It encompasses both cryptography and cryptanalysis.”[73]

Das Online-Lexikon für Informationstechnologie unterscheidet die Formen der Geheimhaltung von Informationen darüber hinaus noch einmal:

„Neben den klassischen kryptographischen Verfahren gibt es auch Verfahren in denen die Nachrichten nicht verschlüsselt, sondern nur in einer anderen Nachricht versteckt werden. Dabei handelt es sich um die Steganografie.“[74]

Zusammenfassend möchte ich versuchen eine Arbeitsdefinition des Begriffes „Kryptologie“ für die hier vorliegende Arbeit aufzustellen:

„Die Kryptologie ist die Wissenschaft der Geheimhaltung von Informationen und Nachrichten, unabhängig von der Art und Weise ihrer Geheimhaltung, sowie der Entschlüsselung, bzw. der Wieder-Sichtbar-Machung dieser Informationen und Nachrichten.“

---

[68] Ertel, Wolfgang: Angewandte Kryptographie, S. 17.
[69] Schneier, Bruce: Angewandte Kryptographie, S. 1.
[70] Bauer, Friedrich: Entzifferte Geheimnisse, S. 2.
[71] http://de.encarta.msn.com/encyclopedia_81501410/Kryptologie.html, letzter Zugriff: 20.03.2009.
[72] http://de.wikipedia.org/wiki/Kryptologie, letzter Zugriff: 20.03.2009.
[73] http://www.britannica.com/EBchecked/topic/145058/cryptology, letzter Zugriff: 21.03.2009.
[74] http://www.itwissen.info/definition/lexikon/Kryptologie-cryptology.html, letzter Zugriff: 20.03.2009.

2. Teilgebiete der Kryptologie

Aus obiger Diskussion und den vielfältigen Definitionen ergibt sich in direkter Weise eine Dreigliedrigkeit der Kryptologie. Sie umfasst nämlich die Teilgebiete Kryptographie, Kryptoanalyse und Steganografie.

2.1. Kryptographie

Die Kryptographie, von den griechischen Begriffen „kryptos“ (= geheim) und „graphein“ (= schreiben) abgeleitet, ist die Lehre oder Wissenschaft der Verschlüsselung von Informationen, also ihrer „Unkenntlich-Machung“.[75] Sie umfasst sämtliche Verfahren und Methoden der Verschlüsselung;[76] dabei wird der ursprüngliche Klartext so verändert, dass in den meisten Fällen der neue Text zwar als „verschlüsselt“ oder „chiffriert“ erkannt wird, er aber nicht (ohne den Aufwand der Entschlüsselung) gelesen werden kann. Kryptographische Verfahren bedürfen sogenannter Schlüssel.[77] Heute hat die Kryptographie, neben ihrem klassischen Feld der Verschlüsselung von Information, auch noch ein zweites Aufgabengebiet, das der Authentifizierung.

2.2. Kryptoanalyse

Der Begriff Kryptoanalyse setzt sich aus „kryptos“ (= geheim), „ana“ (= auf) und „lysys“ (= lösen) zusammen.[78] Sie stellt das Gegenstück zur Kryptographie dar. Ihre Aufgabe ist die Entschlüsselung kryptographischer Verfahren.[79] Diese Aufgabe bezieht sich sowohl auf einzelne Schriftstücke, die, wie uns die Geschichte lehrt, oftmals sehr wichtige Informationen enthalten, was wohl auch ein Grund für deren Verschlüsselung ist. Darüber hinaus gilt die Aufmerksamkeit der Kryptoanalyse aber auch direkt den kryptographischen Verfahren selbst, denn ein Schriftstück zu entziffern ist eine Sache, das ganze System zu „knacken“ und somit in der Folge sämtliche Informationen lesen zu können eine ganz Andere. Dabei verwendet die

[75] http://de.wikipedia.org/wiki/Kryptographie, letzter Zugriff: 21.03.2009.
[76] http://lexikon.meyers.de/wissen/Kryptologie, letzter Zugriff: 21.03.2009.
[77] http://www.britannica.com/EBchecked/topic/145058/cryptology, letzter Zugriff: 21.03.2009.
[78] Wrixon, Fred: Geheimsprachen, S. 17.
[79] http://de.encarta.msn.com/encyclopedia_81501410/Kryptologie.html, letzter Zugriff: 21.03.2009.
http://lexikon.meyers.de/wissen/Kryptologie, letzter Zugriff: 21.03.2009.

Kryptoanalyse nicht den Schlüssel, der bei der Verschlüsselung zum Einsatz kam, denn der steht nur dem Eingeweihten zur Verfügung. Die Kryptoanalyse beschäftigt sich also mit dem „brechen“ der Verfahren ohne Verwendung des Schlüssels.[80] Dabei sucht sie gezielt nach Schwachstellen der Verschlüsselung und bedient sich sämtlicher Informationen, zumeist aus der Analyse des Schlüssels und des Geheimtextes.[81]

2.3. Steganografie

Auch der Begriff der Steganografie ist griechischen Ursprungs, er kommt von „steganos“ (= schützend, bedeckt) und „graphein“ (= schreiben).[82] Im Gegensatz zur Kryptographie ist es aber nicht Ziel der Steganografie Informationen unkenntlich zu machen, sondern diese direkt zu verstecken, sodass ein Uneingeweihter deren Existenz nicht bemerkt.[83] Auf diesem Umstand beruht auch der gesamte Sicherheitsfaktor steganografischer Methoden. Während kryptographische Verfahren zumeist der Kryptoanalyse bedürfen um wieder lesbar gemacht zu werden, kann bei der Mehrheit der steganografischen Verfahren auch der Laie diese sofort auslesen, wenn sie entdeckt wurden. Der Vorteil der Steganografie gegenüber der Kryptographie besteht allerdings darin, dass, aufgrund der Unkenntnis Dritter, eine konkrete Untersuchung auf steganografische Inhalte meist ausbleibt. Dennoch gibt es analog zu Kryptographie und Kryptoanalyse auch zur Steganografie einen „Gegenspieler“, der sich mit der Aufdeckung solcher Inhalte beschäftigt, die Steganalyse.[84]

3. Grundbegriffe

Wie jedes andere Gebiet hat auch die Kryptologie ihre Fachbegriffe. Eigentlich wollte ich diesen Teil der Arbeit der Kryptographie voranstellen, da die hier erklärten

[80] http://www.britannica.com/EBchecked/topic/145058/cryptology, letzter Zugriff: 21.03.2009.
[81] http://de.wikipedia.org/wiki/Kryptoanalyse, letzter Zugriff: 21.03.2009.
http://www.itwissen.info/definition/lexikon/Kryptoanalyse-crypto-analysis.html, letzter Zugriff: 21.03.2009.
[82] http://de.wikipedia.org/wiki/Steganografie, letzter Zugriff: 21.03.2009.
[83] Schmeh, Klaus: Versteckte Botschaften, S. 3.
http://de.wikipedia.org/wiki/Steganografie, letzter Zugriff: 21.03.2009.
http://www.itwissen.info/definition/lexikon/Steganografie-steganography.html, letzter Zugriff: 21.03.2009.
[84] http://de.wikipedia.org/wiki/Steganografie, letzter Zugriff: 21.03.2009.

Begriffe Grundlagen der Kryptographie darstellen, allerdings hatte ich bei der Erarbeitung der geschichtlichen Entwicklung der Kryptologie ziemliche Mühe diese Begriffe zu umgehen, bzw. es ist mir nicht immer gelungen, sodass ich zu dem Ergebnis gekommen bin, dass es für alle Beteiligten leichter wird, wenn ich die folgenden Grundbegriffe bereits an dieser Stelle erkläre und diese anschließend verwenden kann.

3.1. Transposition

Die Transposition bedeutet die Verschlüsselung von Nachrichten mittels Verschiebung der einzelnen Buchstaben, Zeichen oder Symbole. Es findet also lediglich eine Vertauschung der Stelle statt, anders ausgedrückt: Die Reihenfolge der Buchstaben verändert sich. Alle Verfahren bei denen die Botschaft dadurch verschlüsselt wird, dass die einzelnen Elemente ihre Reihenfolge ändern (also z.B. die weiter unten beschrieben Verfahren der Skytale von Sparta oder das Verfahren nach Fleissner) werden als Transpositionschiffren bezeichnet.

3.2. Substitution

Die Substitution bildet in der Kryptographie die zweite wichtige Gruppe von Verschlüsselungsmethoden. Substitutionsverfahren verändern nicht die Reihenfolge der Zeichen, sie verändern die Zeichen selbst, indem sie diese durch andere Zeichen ersetzen. Die Reihenfolge der Buchstaben bleibt dabei gleich. Innerhalb der Substitutionschiffren unterscheidet man noch einmal in monoalphabetische und polyalphabetische Substitutionen. Bei monoalphabetischen Substitutionen wird zur Verschlüsselung ein Alphabet herangezogen, sodass eine bijektive Zuordnung zwischen den Buchstaben des Klartextalphabetes und denen des Geheimtextalphabetes vorgenommen wird. Der Klartextbuchstabe wird dann jeweils durch sein Pendant im Geheimtextalphabet ersetzt. Eine polyalphabetische Substitution verwendet hingegen viele, mindestens jedoch zwei, unterschiedliche Geheimtextalphabete. Durch die Abwechslung zwischen den unterschiedlichen Geheimtextalphabeten wird ein höheres Maß an Sicherheit erzielt.

3.3. Symmetrische – asymmetrische Verschlüsselung

Die Bezeichnungen symmetrische und asymmetrische Verschlüsselung beschreiben die beiden Hauptrichtungen der Kryptographie. Bei der symmetrischen Verschlüsselung wird ein Schlüssel generiert, der sowohl zur Ver- als auch zur Entschlüsselung verwendet wird. Man begibt sich also auf einem Weg vom Klartext zum verschlüsselten Text über den Schlüssel hin und auf dem gleichen Weg über den gleichen Schlüssel auch wieder zum Klartext zurück. Man verschlüsselt also symmetrisch.
Bei der asymmetrischen Verschlüsselung werden zwei unterschiedliche Schlüssel erzeugt, von denen der eine ausschließlich der Verschlüsselung dient und der andere ausschließlich der Entschlüsselung. Der Weg vom Klartext zum Geheimtext ist also ein anderer, als der Weg zurück. Es wird also entsprechend asymmetrisch verschlüsselt.

4. Die geschichtliche Entwicklung der Kryptologie

Eine Arbeit, die sich das genetische Prinzip zugrunde legt, kann sich nicht darauf beschränken eine Aufzählung und Beschreibung kryptographischer Verfahren darzustellen. Sie muss darüber hinaus einen Abschnitt zur gesamten Entwicklung der Kryptologie beinhalten, denn es waren gerade oftmals die Kryptoanalytiker, die solche Verfahren brachen und damit die Entwicklung neuer Methoden erzwangen. Auch ihnen muss hier Rechnung getragen werden und ich möchte nur noch einmal an den Satz von Otto Toeplitz erinnern:

> *„Wenn man an diese Wurzeln der Begriffe zurückginge, würden der Staub der Zeiten, die Schrammen langer Abnutzung von ihnen abfallen, und sie würden wieder als lebensvolle Wesen vor uns entstehen.“*[85]

Es ist mir zwar nicht möglich den Suchprozess nach den einzelnen Verfahren darzustellen, dennoch ist der folgende Abschnitt dieser Arbeit der Geschichte der Kryptologie gewidmet. Dabei soll auf eine ausführliche Darstellung der kryptographischen Verfahren weitgehend verzichtet werden. Es soll im Folgenden eher um die Umstände, Persönlichkeiten und Entwicklungen, sowie deren Zusammenspiel in der Geschichte gehen. Weitere interessante, aber für diese Arbeit

[85] Toeplitz, Otto, zitiert in: Wittmann, Erich: Grundfragen des Mathematikunterrichts, S. 133.

wenig relevante, geschichtliche Entwicklungen befinden sich im Anhang zu dieser Arbeit.

4.1. Vorchristliche Zeit (ca. 4000 v. Chr. – 0)

4.1.1. Die ägyptischen Hieroglyphen (ca. 4000 v. Chr.)

Die Hieroglyphen der alten Ägypter stellen uns heutzutage vor so manches Rätsel. Mit ihrer Darstellung in Symbolen sehen sie auch aus wie geheime Zeichen, allerdings waren diese Hieroglyphen die Schrift der Ägypter. Wenn wir sie also als Geheimschrift betiteln, müssten wir dies auch mit sämtlichen in Fremdsprachen geschrieben Texten tun, die uns nicht geläufig sind und wir müssten uns darüber im Klaren sein, dass Menschen mit anderen Muttersprachen auch deutsche Texte als Geheimschrift ansehen. Unter Berücksichtigung des grundlegenden Codierungsaspekts von Buchstaben und Schrift wäre dies zwar grundsätzlich tragbar, allerdings käme kein Mensch auf die Idee Texte in seiner Muttersprache als Geheimschrift anzusehen. Wieso sollte er das auch tun? Es fehlt ihnen ja gerade der Verschlüsselungsaspekt. Um die reinen Hieroglyphen geht es hier aber auch überhaupt nicht. Tatsächlich geben Historiker an, dass die Schreiber von Texten auf Monumenten und Grabmälern von Herrschern im alten Ägypten, den Hieroglyphen besondere Formen gaben, um sie von den einfachen Menschen abzuheben und somit als etwas Besonderes zu charakterisieren.[86] Aufgrund des fehlenden Verschlüsselungsaspektes, denn die Hieroglyphen blieben ja grundsätzlich gleich, mag man hier den Begriff Kryptographie vielleicht gar nicht recht verwenden, doch Wrixon führt weiter aus, dass dieser Veränderung zwei kryptologische Prinzipien zugrunde liegen:

> *„[…] nämlich der Transformation von Schrift und der Geheimhaltung dieses Vorgangs.“*[87]

4.1.2. Geheimschriften in Mesopotamien (ca. 1500 v. Chr.)

Das erste echte Zeugnis kryptographischer Kunst, das wir heute kennen, stammt aus Mesopotamien aus der Zeit um 1500 v. Chr. Die damals dort lebenden Völker

[86] Wrixon, Fred: Geheimsprachen, S. 17.
[87] Wrixon, Fred: Geheimsprachen, S. 18.

verwandten Keilschriften zum Festhalten und zur Weitergabe von Informationen und Nachrichten. Aus dieser Zeit stammt eine Tabelle mit einem Rezept zur Herstellung einer speziellen Tonglasur. Während der Inhalt dieses Rezeptes damals etwas Besonderes gewesen sein muss, ist es heute das Rezept selbst, oder besser gesagt, die Art wie dieses Rezept aufgeschrieben wurde; so wurden die Zeichen der Inhaltsstoffe absichtlich durcheinander gebracht, um die genaue Rezeptur geheim zu halten.[88]

4.1.3. Atbash (ca. 600 v. Chr.)

Atbash ist eine Geheimschrift, die etwa 600 v. Chr. in Palästina angewendet wurde.[89] Sie sieht eine Vertauschung der hebräischen Buchstaben vor (wie genau das funktioniert wird später erklärt). Diese Geheimschrift ist insbesondere durch die Bibel bekannt geworden. Dort findet sie im Alten Testament im Buch Jeremia Anwendung, wo der Name Babel durch Scheschach ersetzt wird. Da im Folgesatz Babel wieder im „Klartext“ geschrieben steht, liegt der Anwendung in der Bibel offensichtlich kein Verschlüsselungsmotiv zugrunde.[90]

4.1.4. Indische Geheimschriften (ca. 500 v. Chr.)

Seit etwa 500 v. Chr. wurden Geheimschriften in Indien bereits erstaunlich professionell eingesetzt. Die Inder kannten verschiedene Methoden von der Vertauschung von Buchstaben bis hin zu verschiedenen schiefen Schreibstilen. Anwendung fanden Geheimschriften im Informationsaustausch zwischen Spionen, sowie bei Frauen, zumindest wurde ihnen das im Kamasutra empfohlen.[91] Tatsächlich enthält das, heute vor allem für seinen erotischen Bereich bekannte, Kamasutra von Vatsjajana eine Liste von 64 Künsten, die Frauen studieren sollten, darunter auch Mlecchita-vikalpa, die Kunst der Geheimschrift, um ihre Affären zu verbergen.[92] Darüber hinaus wird auch eine Anleitung für eine mögliche Methode gegeben. Sie sieht vor, dass man die Buchstaben des Alphabets zufällig miteinander

[88] Wrixon, Fred: Geheimsprachen, S. 18.
[89] http://de.wikipedia.org/wiki/Atbash, letzter Zugriff: 21.03.2009.
[90] Wrixon, Fred: Geheimsprachen, S. 19.
[91] Wrixon, Fred: Geheimsprachen, S. 18.
[92] Singh, Simon: Geheime Botschaften, S. 24.

paart und den jeweiligen Buchstaben im Klartext durch seinen Partner ersetzt.[93] Allein diese Anleitung liefert für unser lateinisches Standartalphabet (also ohne Sonderzeichen) immerhin 26! Möglichkeiten, wenn man außer Betracht lässt, dass es wenig Sinn macht einen Buchstaben mit sich selbst zu vertauschen. Das Kamasutra wurde zwar erst im 4. Jahrhundert n. Chr. verfasst, allerdings geht es auf Handschriften aus dem 4. Jahrhundert v. Chr. zurück.

4.1.5. Die Kryptologie der Spartaner (ca. 500 v. Chr.)

Die Kryptographie erlebte in der Geschichte immer wieder Blütezeiten während Kriegen. Das ist nicht weiter verwunderlich, wenn man bedenkt, dass es gerade in Kriegszeiten von enormer Bedeutung ist, dass der Gegner über die eigenen Taktiken keine Informationen hat. Das wahrscheinlich erste kryptographische Verfahren, dass zu Kriegszwecken verwendet wurde, wird den Spartanern zugeschrieben.[94] Im griechisch-persischen Konflikt verwendeten sie im 5. Jahrhundert v. Chr. die sogenannte Skytale, eine Verschlüsselung, bei der mit Hilfe eines Holzstabes und eines Pergamentstreifens die Buchstabenposition innerhalb eines Textes verändert und der Inhalt somit unkenntlich gemacht wurde (Eine genauere Betrachtung der Methode der Skytale folgt später). Darüber hinaus wurde der Pergamentstreifen von den Boten oftmals an der Innenseite ihres Gürtels befestigt, sodass ein kryptographisches und ein steganografisches Verfahren kombiniert wurden.[95]
404 v. Chr. gelang es einem einzigen von fünf Boten von Persien nach Sparta zu marschieren und General Lysander von Sparta seinen Gürtel zu überreichen. Der wickelte die darin enthaltene Botschaft auf seine Skytale und erfuhr sogleich, dass Pharnabasus von Persien einen Angriff auf Sparta plante.[96]
Zur damaligen Zeit waren steganografische Verfahren weiter verbreitet als kryptographische. Neben dem Einsatz der Skytale verwendeten die Spartaner z.B. Wachstafeln zum Schreiben oder Tiermägen um Nachrichten zu verbergen.[97]

[93] Singh, Simon: Geheime Botschaften, S. 24.
[94] Singh, Simon: Geheime Botschaften, S. 23.
[95] Singh, Simon: Geheime Botschaften, S. 24.
[96] Singh, Simon: Geheime Botschaften, S. 24.
[97] Wrixon, Fred: Geheimsprachen, S. 22.

4.1.6. Die Rauch- und Fackelsignale der Griechen (ca. 4. Jahrhundert v. Chr.)

Eine große Rolle spielten in der damaligen Zeit auch Rauch- und Fackelsignale. Insbesondere in Griechenland wurden solche Methoden verwendet um Informationen zu übermitteln. In den meisten Fällen dienten diese Verfahren aber dazu die Information auf visuellem Wege über größere Distanzen zu versenden und weniger der Geheimhaltung. Sehr oft wurden solche Signale auch an Küstengebieten aufgestellt um Schiffe vor Sandbänken zu warnen.[98]

4.1.7. Polybios (2. Jahrhundert v. Chr.)

Polybios war ein griechischer Historiker, der im 2. Jahrhundert v. Chr. lebte. Sein Hauptwerk war die Universalgeschichte Roms vom ersten punischen Krieg bis zur Zerstörung Karthagos und Korinths in 40 Bänden.[99] Daneben befasste er sich aber auch mit Geheimschriften und entwickelte eine Methode, die noch heute als Schachbrett des Polybios[100] oder Polybios-Tafel[101] bekannt ist.

4.1.8. Julius Caesar (1. Jahrhundert v. Chr.)

Julius Caesar lebte im 1. Jahrhundert v. Chr. Er war ein römischer Staatsmann und wurde später Prokonsul, bevor er sich zum Alleinherrscher des römischen Reiches ausrief. Da er die Ausdehnung des Reiches zum Ziel hatte, war seine Regentschaft von Kriegen geprägt, daher war es für ihn von großer Bedeutung seine Nachrichten nicht ungeschützt durch die Kriegsgebiete zu senden. Er verwandte verschiedene Signalstationen, ähnlich denen der Griechen. Außerdem beschreibt er in seinem Werk „Commentarii de bello gallico“ (zu Deutsch: Kommentare über den gallischen Krieg) wie er selbst für seine lateinischen Nachrichten griechische Buchstaben verwendet.[102] Sein bedeutendstes kryptographisches Wirken aber, bestand in der Verwendung einer Methode die noch heute seinen Namen trägt: das Caesar-Verfahren.[103] Dieses Verfahren verwandte er bei der Konversation mit Quintus

[98] Wrixon, Fred: Geheimsprachen, S. 22.
[99] Kippenhahn, Rudolf: Verschlüsselte Botschaften, S. 161.
[100] Wrixon, Fred: Geheimsprachen, S. 22 f.
[101] Kippenhahn, Rudolf: Verschlüsselte Botschaften, S. 161.
[102] Wrixon, Fred: Geheimsprachen, S. 23.
[103] Singh, Simon: Geheime Botschaften, S. 25.

Cicero, der mit seinen Männern belagert, kurz davor war sich zu ergeben. Caesar schreibt selbst:

> *„Wenn (der gallische Bote) nicht persönlich herankommen könne, solle er, wie ich ihm riet, einen Wurfspieß mit dem am Wurfriemen befestigten Brief in das Lager schleudern […] Aus Furcht vor der Gefahr schleuderte der Gallier auftragsgemäß den Wurfspieß hinein. Dieser blieb durch Zufall in einem Turme stecke, wurde zwei Tage lang von niemandem bemerkt. Erst am dritten Tag sah ein Soldat den Brief, nahm ihn ab und brachte ihn Cicero. Er las die Mitteilung, gab sie dann den Soldaten bekannt und löste größte Freude im Lager aus.“*[104]

4.2. Das Mittelalter (ca. 500 n. Chr. bis 1500 n. Chr.)

Im dunklen Mittelalter war es nur in Europa dunkel, dennoch entstand eine interessante Substitutionschiffre. Außerdem erblickte das erste Buch zur Kryptologie nicht im dunklen Teil der Erde, sondern im arabischen Raum, das Licht der Welt.

4.2.1. Alphabetum Kaldeorum

Der Name Alphabetum Kaldeorum geht auf das Volk der Chaldäer zurück. Wie der Name vermuten lässt, handelt es sich um ein Alphabet mit Zeichen, welche die Klartextzeichen ersetzen sollen. Die Alphabetstafel selbst lässt darauf schließen, dass das Verfahren auf lateinische Schriften angewendet wurde, denn „u“ und „v“ werden gleich verwendet, „j“ fehlt gänzlich und „w“ wird als zwei „v“ geschrieben. Um einer Häufigkeitsanalyse vorzubeugen gab es für einige häufige Buchstaben auch zwei unterschiedliche Zeichen. Zusätzlich wurden in die chiffrierten Texte oft sinnlose Zeichen eingeschoben um das entschlüsseln unbefugter zusätzlich zu erschweren.[105]

[104] Singh, Simon: Geheime Botschaften, S. 25.
[105] http://www.vision-ing21.de/downloads/6.geschichtederkryptographie.pdf, letzter Zugriff: 21.03.2009.

4.2.2. Erstes Buch zur Kryptologie

Eines sollte man nicht vergessen, das dunkle Mittelalter fand hauptsächlich in Europa statt. Die Araber machten zu dieser Zeit große Fortschritte in der Kryptologie.
855 n. Chr. wurde im arabischen Raum die erste schriftliche Abhandlung über Kryptologie veröffentlicht. Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi beschreibt in seinem Werk „Abhandlung über die Entzifferung kryptographischer Botschaften", wie es ihm gelungen war eine Nachricht an einen byzantinischen Kaiser zu dechiffrieren. Die Methode, die er dafür verwendete, sollte noch lange nach ihm in der Kryptoanalyse praktiziert werden: die Häufigkeitsanalyse.[106]

4.3. Die Renaissance (ca. 14 Jh. bis Ende 16 Jh. n. Chr.)

4.3.1. Die Geheimschrift des Vatikan (ca. 1300 n. Chr.)

Die Anfänge der Renaissance waren noch sehr stark mittelalterlich geprägt. Aus Angst vor einer Anklage nutzten immer mehr Personen Geheimschriften für ihre Korrespondenz.[107] Der expandierende Katholizismus ging zunächst dagegen vor, nachdem sich die Kirche aber vermehrt in Disputen mit den weltlichen Oberhäuptern befand, hielten sie es für angemessen, ihre eigenen Nachrichten zu verschlüsseln. Dabei ersetzten Sekretäre des Vatikans zunächst ganze Namen durch einzelne Buchstaben. Gegen Ende des 14. Jahrhunderts war dieses System zu einem umfassenden Verschlüsselungssystem herangereift. Es bestand aus Kombination ganzer Tabellen mit Codewörtern für Namen, Wörter oder Silben, sowie Listen von Geheimschriftalphabeten die benutzt wurden um die Buchstaben zu ersetzen. Diese Art der Verschlüsselung nannte man Nomenklator, abgeleitet aus den lateinischen Begriffen „nomen" (= Name) und „calator" (= Rufer).[108]

---

[106] Singh, Simon: Geheime Botschaften, S.33 f.
[107] http://www.vision-ing21.de/downloads/6.geschichtederkryptographie.pdf, letzter Zugriff: 21.03.2009.
[108] Wrixon, Fred: Geheimsprachen, S. 24.

4.3.2. Leon Alberti (15. Jh. n. Chr.)

Leon Battista Alberti wurde 1404 in Genua geboren und war eine der herausragendsten Persönlichkeiten seiner Zeit. Die Vielfältigkeit seiner Begabungen ist erstaunlich. Bei Wikipedia ist zu lesen:

> *„Leon Battista Alberti war ein italienischer Humanist, Schriftsteller, Mathematiker, Kryptologe, Architekt und Architekturtheoretiker der Renaissance.“*[109]

Doch damit nicht genug. Simon Singh zeigt in seinem Buch weitere Tätigkeitsfelder des Italieners auf:

> *„[…]: Maler, Komponist, Dichter und Philosoph sowie Verfasser der ersten wissenschaftlichen Analyse der Perspektive, […]“*[110]

Bis Alberti auf den Plan trat, hatten sich kryptographische Verfahren mehrere Jahrhunderte mit einem Geheimschriftalphabet begnügt und die Klartextzeichen monoalphabetisch verändert. Dieses Verfahren war aber seit der Häufigkeitsanalyse unsicher geworden. Alberti war der Erste, der auf die Idee kam zwei oder mehr Geheimschriftalphabete zu verwenden und beim Verschlüsseln zwischen ihnen abzuwechseln (den ersten Buchstaben der Nachricht mit dem ersten Alphabet verschlüsseln, den zweiten Buchstaben mit dem zweiten Alphabet, den Dritten wiederum mit dem ersten Alphabet, usw.) um die Kryptoanalytiker zu verwirren. Damit legte er den Grundstein der polyalphabetischen Verschlüsselung.[111] Darüber hinaus konstruierte Alberti eine Verschlüsselungsscheibe, die der von Caesar sehr ähnlich war. Alberti besaß allerdings den Weitblick die Stellung der Scheiben zueinander während der Verschlüsselung zu verändern.

4.3.3. Johannes Trithemius (Ende 15. – Anfang 16. Jh. n. Chr.)

Johannes Trithemius wurde als Johannes Heidenberg in Trittenheim an der Mosel geboren. Der Name Trithemius, wie er sich selbst später nannte, entspricht der lateinischen Schreibweise seines Geburtsortes. Eigentlich war Trithemius ein deutscher Klosterabt, doch auch er war, ähnlich wie Alberti, wenn auch vielleicht nicht ganz so umfassend, ein vielseitiger Gelehrter. Er schrieb über 90 Bücher, die

[109] http://de.wikipedia.org/wiki/Leon_Battista_Alberti, letzter Zugriff: 22.03.2009.
[110] Singh, Simon: Geheime Botschaften, S. 65.
[111] Singh, Simon: Geheime Botschaften, S. 65 f.

meisten davon hatten einen kirchlichen Hintergrund, doch unter ihnen war auch die „Polygraphiae libri sex“ (zu Deutsch: Sechs Bücher zur Polygraphie), das erste gedruckte Werk zur Kryptographie überhaupt.[112] Darin enthalten ist die „Recta transpositionis tabula“ (zu Deutsch: Regelmäßig umgesetzte Tabelle) heute eher unter der kürzeren Version „Tabula Recta“ bekannt. Dabei handelt es sich um ein Quadrat aus (in der Originalversion) 24 x 24 Buchstaben („u“ und „v“, sowie „i“ und „j“ wurden in der lateinischen Sprache nicht unterschieden). Die erste Zeile ist dabei das Standartalphabet, jede Zeile untendrunter ist dabei um jeweils einen Buchstaben nach vorne verschoben (die zweite Zeile beginnt also mit dem Buchstaben „b“, die Dritte mit „c“, usw.). Die Verschlüsselung mit Hilfe der Tafel erfolgt dann regelmäßig, ähnlich wie bei Alberti: Der erste Buchstabe wird mit dem ersten Alphabet verschlüsselt, der Zweite mit dem zweiten, der Dritte mit dem Dritten, usw. Trithemius Tabula recta stellt eine Verfeinerung von Albertis Verfahren dar.[113]

4.3.4. Giovanni Battista della Porta (16. – 17. Jh. n. Chr.)

Auch der Italiener Giovanni Battista della Porta gehörte zu den typischen Universalgelehrten der Renaissance. Sein wahrscheinlich bekanntestes Werk ist die „Magia naturalis“, ein Kompendium aus 20 Büchern, das sich mit unterschiedlichsten Themen beschäftigt. Eine komplette Übersetzung des lateinischen Textes ins Englische befindet sich im Internet. Das sechzehnte Buch trägt den Titel „Of invisible writing“ und beschreibt in dreizehn Kapiteln verschiedene steganografische Methoden[114], darunter mehrere Methoden wie man Nachrichten in einem gekochten Ei versteckt. Eine davon lautet:

> *„Man mische eine Unze Alaun in einen Becher Essig und schreibe mit dieser Tinte auf die Eischale. Die Lösung dringt durch die poröse Schale und hinterlässt eine Botschaft auf der Oberfläche des gehärteten Eiweißes, die nur dann gelesen werden kann, wenn die Schale entfernt wird.“*[115]

Fünf Jahre nach der „Magia naturalis“ erschien ein Buch von Porta mit dem Titel „de furtivis literarum notis“ (etwa: „Anmerkungen über versteckte Botschaften“), ein Werk,

[112] http://de.wikipedia.org/wiki/Trithemius, letzter Zugriff: 22.03.2009.
[113] http://de.wikipedia.org/wiki/Tabula_recta, letzter Zugriff: 22.03.2009.
[114] vgl. http://homepages.tscnet.com/omard1/jportat2.html, letzter Zugriff: 22.03.2009.
[115] Porta, Giovanni Battista, zitiert in Singh, Simon: Geheime Botschaften, S. 20.

das sich ausschließlich dem Gebiet der Kryptographie widmete. Darin beschreibt er das erste digraphische Verschlüsselungsverfahren, bei dem nicht mehr einzelne Zeichen einer Nachricht ersetzt werden, sondern Zeichenpaare. Außerdem beinhaltet das Buch einen weiteren Schritt der Entwicklung polyalphabetischer Verschlüsselungen. Die nach ihm benannte Porta-Chiffre verwendet dreizehn unterschiedliche Alphabetpaarungen. Porta verwendet dafür bereits ein Schlüsselwort. Die einzelnen Buchstaben dieses Schlüsselwortes bestimmen die jeweiligen Alphabetpaarungen. Der Buchstabe des Klartextes wird dann seinem dortigen Partner zugeordnet.[116]

4.3.5. Blaise de Vigenère (16 Jh. n. Chr.)

Blaise de Vigenère wurde 1523 in Saint-Purçain geboren. Er war zunächst französischer Diplomat und begegnete den Abhandlungen Albertis, Trithemius‘ und Portas im Alter von sechsundzwanzig Jahren auf einer diplomatischen Mission in Rom. Zu dieser Zeit konnte er sich wegen seiner Beschäftigung nur oberflächlich damit beschäftigen. Sein Interesse an der Kryptographie war praktisch geprägt. Nachdem er im Alter von neununddreißig Jahren der Meinung war genügend Vermögen angehäuft zu haben, widmete er sich fortan der Wissenschaft. Er studierte die Schriften Albertis, Trithemius‘ und Portas noch einmal, diesmal intensiver und schließlich gelang es ihm ein eigenes, sehr sicheres, polyalphabetisches Verfahren zu gestalten (das immerhin erst über 250 Jahre später zum ersten Mal geknackt wurde). 1585 veröffentlicht er sein Buch „Traicte de Chiffres“, eine Arbeit die sich mit der Kryptographie befasst und zu seinen bekanntesten Werken zählt. Dort beschreibt er das Verfahren, das zu seinen Ehren noch heute seinen Namen trägt: die Vigenère-Verschlüsselung.[117]

Diese Methode verwendet eine Vigenère-Tafel (oder auch Vigenère-Quadrat genannt), die der Tabula Recta von Trithemius gleicht. Im Gegensatz zu Trithemius verwendet Vigenère die Tafel aber nicht regelmäßig, sondern kombiniert sie mit der Idee Portas ein Schlüsselwort zu verwenden. Eine genauere Erklärung des Verfahrens folgt später.

---

116 http://www.kryptographiespielplatz.de/index.php?aG=d47be41482870a3cfb900dbd5b223a552f2ada24&PHPSESSID=46l17g4pt5aocssss793reil34, letzter Zugriff: 22.03.2009.

117 Singh, Simon: Geheime Botschaften, S. 68.

4.3.6. Das Babington-Komplott (16. Jh. n. Chr.)

Das 16. Jh. war in England von einer Spannung zwischen Katholiken und Protestanten geprägt. Diese Spannung erreichte Ende der 50er Jahre dieses Jahrhunderts ihren Höhepunkt in einem Gerichtsverfahren und anschließendem Urteil, das die Welt nicht vergessen würde und in dem Geheimschriften die zentrale Rolle spielten. Der Zwist zwischen Katholiken und Protestanten wurde auf allen gesellschaftlichen Ebenen, bis hin zur königlichen, ausgetragen. 1558 bestieg Königin Elisabeth I., eine Protestantin, den englischen Thron. In Schottland regierte Maria Stuart, eine Katholikin. Die Streitigkeiten der damaligen Zeit führten zu allerhand Gerüchten über Pläne Elisabeth I. abzusetzen und Maria Stuart zur Königin von England zu machen. Das führte dazu, dass Königin Elisabeth I. eine Schar treuer Gefolgsleute um sich versammelte, darunter eine Einheit von ca. 50 Mann, die nur den Auftrag hatten die innere Sicherheit zu gewährleisten. Zum Minister für innere Sicherheit ernannte Elisabeth I. Sir Francis Walsingham.
Walsingham wurde um 1530 in Kent geboren und studierte ab 1548 am King's College in Cambridge. Er befasste sich intensiv mit fremden Ländern, ihren Sprachen und diplomatischen Gebräuchen. 1550 ging er ins Ausland. 1552 kehrte er zurück und begann ein Studium der Rechtswissenschaften in Gray's Inn in London. Nach dem Tod König Eduards VI. verließ er England erneut, um sein Studium in Padua fortzusetzen. Später führte ihn sein Weg auch noch für zwei Jahre in die Schweiz. Während seiner Aufenthalte auf dem europäischen Festland knüpfte er zahlreiche Kontakte, die ihm als Minister für innere Sicherheit später noch einmal sehr hilfreich werden sollten. Walsingham kehrte erst mit der Ernennung der protestantischen Elisabeth I. zur Königin nach England zurück.[118]
Walsingham verstand es in seinem Amt als Minister wie kaum ein zweiter die Fähigkeiten seiner Mitarbeiter zu erkennen und sie, diesen entsprechend, gewinnbringend einzusetzen. Sein Amt versetzte Walsingham in die Lage eine Liste all jener Personen anzulegen, die Elisabeth I. gefährlich werden konnten. Die Liste wurde von Maria Stuart angeführt. Maria Stuart und Elisabeth I. waren Cousinen und da Elisabeth I. keine Kinder hatte, war Maria Stuart Elisabeths rechtmäßige Thronfolgerin. Nachdem Maria Stuart großes Pech mit ihren Ehemännern gehabt

[118] http://de.wikipedia.org/wiki/Francis_Walsingham, letzter Zugriff: 23.03.2009.

hatte (der Erste starb, der Zweite wurde ermordet und der Dritte floh) wurde sie von einigen Aristokraten gezwungen Schottland zu verlassen, was sie auch tat. Sie suchte daraufhin bei ihrer Cousine Elisabeth Schutz und Zuflucht, was diese ihr auch gewährte, doch aufgrund der von ihr ausgehenden Gefahr für Elisabeth, konnte Walsingham dafür sorgen, dass Maria Stuart während ihres Aufenthaltes in England immer strenger in Gewahrsam genommen wurde, die gegen Ende einer Gefangenschaft gleich kam. Während dieser Zeit avancierte Maria Stuart zum Symbol der Katholiken, die sich von der protestantischen Elisabeth I. unterdrückt fühlten. Walsinghams Männer teilten ihm mit, dass Bestrebungen im Gange seien Maria Stuart zur Königin von England zu krönen. Dies setzte voraus, dass Elisabeth I. sterben musste. Walsingham wollte Elisabeth I. und den Protestantismus schützen und entschied sich diesen Bestrebungen die Grundlage zu nehmen. Er wollte Maria Stuart wegen Hochverrats an der Krone überführen, worauf die Todesstrafe stand. Ohne Maria Stuart hatten ihre katholischen Gefolgsleute keine Chance den Katholizismus als Staatsreligion durchzusetzen. Doch Elisabeth I. forderte eindeutige Beweise für Marias Schuld und das aus gutem Grund, denn Maria Stuart war eine schottische Königin und es gab viele Zweifler, ob ein englisches Gericht überhaupt in der Lage war ein ausländisches Staatsoberhaupt zum Tode zu verurteilen, außerdem wollte Elisabeth I. keinen Präzedenzfall schaffen, der eben diese Erlaubnis erteilt, denn sie hatte Angst, dass die Streitigkeiten zwischen Katholiken und Protestanten dazu führen könnten, dass der englische Staat in der Folge auch andere Staatsoberhäupter töten lassen würde, oder sich zumindest dazu in der Lage sah, allen voran sie selbst. Die Blutsverwandtschaft beider verstärkte das Dilemma noch. Walsingham musste also eindeutige, unwiderlegbare Beweise dafür vorlegen, dass Maria Stuart von diesen Verschwörungen wusste und darüber hinaus selbst darin verstrickt war.[119] In der Folge versammelte Walsingham eine Schar von Verschwörern um sich, darunter der erste bedeutende Kryptoanalytiker Englands Thomas Phelippes.

Anthony Babington, der dieser Verschwörung seinen Namen gab, war Katholik und finanziell gut situiert. Diese Voraussetzungen hatten in ihm einen Plan gedeihen lassen, der tatsächlich den Sturz der Königin und die Befreiung sowie Erhebung zur neuen Königin Maria Stuarts vorsah. Er und seine Komplizen, darunter der katholische Priester John Ballard, suchten nach Unterstützung für ihren Plan in

[119] Singh, Simon: Geheime Botschaften, S. 15 ff.

Frankreich und Spanien. Ihr Plan war kompliziert: Ermordung Elisabeths und einiger ihrer wichtigen Minister, Befreiung von Maria aus Chartley Castle, wo sie gefangen gehalten wurde, sowie die Kaperung sämtlicher Schiffe der Royal Navy zur Überwachung der Themse und die Bewaffnung aller Katholiken. Mit Hilfe von Philipp II. von Spanien wollten sie dann die protestantische Monarchie stürzen und Maria Stuart zur Königin machen.[120]

Doch Walsingham schleuste einen Spion in die Reihen von Babington: Gilbert Gifford. Gifford gehörte einer prominenten katholischen Familie an und sollte eigentlich Priester werden, doch er hatte sich etwas zu Schulden kommen lassen und ihm drohte eine Gefängnisstrafe. Als einflussreicher Minister legte Walsingham Fürsprache ein und Gifford blieb das Gefängnis erspart, dafür schlug er sich auf die Seite Walsinghams. Gifford ging daraufhin als katholischer Mönch nach Chartley Castle und bot Maria dort seine Hilfe beim Austausch geheimer Botschaften an, außerdem schürte er in Babington die Glut der Verschwörung, die diesen schließlich zu obigem Plan veranlasste. Die geheimen Nachrichten an und von Maria Stuart wurden im Spund eines Bierfasses nach Chartley Castle (und von dort weg) transportiert. Gifford entnahm die Nachricht dem Spund und schickte einen Helfer mit ihr zu Maria, diese entnahm die Nachricht aus dem Lederumschlag und legte ihre eigene hinein, die dann im Spund eines leeren Bierfasses aus Chartley Castle abtransportiert wurde. Doch Gifford fing sämtliche Nachrichten ab, er konnte nur nichts damit anfangen, da Maria Stuart vorsichtig genug war ihre eigenen Briefe zu verschlüsseln. Also übergab Gifford die Briefe an den Kryptoanalytiker Thomas Phelippes.[121]

Als Maria Stuart am 15. Oktober 1586 den Richtern vorgeführt wurde, sollte ihr Schicksal von ihrer eingesetzten Geheimschrift bestimmt werden. Die Tatsache, dass sie angeklagt wurde, ließ sie vermuten, dass ihre Briefe gefunden worden waren, doch da Maria diese ja verschlüsselt hatte, glaubte sie, dass die Ankläger nichts gegen sie in der Hand hatten. Ihr Leben hing also schließlich davon ab, ob es Thomas Phelippes gelungen war ihre Geheimschrift zu entschlüsseln oder nicht. Maria hatte zur Verschlüsselung ihrer Briefe einen Nomenklator, bestehend aus griechischen Buchstaben, Zahlen und Symbolen verwendet. Zu ihrem Verhängnis wurde allerdings, dass sie die Arbeiten von Alberti, Trithemius, Porta oder Vigenère nicht kannte und ihre Buchstaben somit monoalphabetisch verschlüsselte. Phelippes

[120] Wrixon, Fred: Geheimsprachen, S. 30 ff.
[121] Wrixon, Fred: Geheimsprachen, S. 30 ff.

hatte keine Probleme damit gehabt ihre Geheimschrift zu knacken. Sie wurde des Hochverrats für schuldig befunden und am 8. Februar 1587 enthauptet.
Darüber hinaus ließ Walsingham einen Brief an Babington fälschen in dem Maria angeblich die Namen seiner Komplizen wissen wollte. Damit gelang es Walsingham auch die Verschwörer gefangen zu nehmen und ebenfalls zum Tode zu verurteilen.[122]

4.4. Vorindustrielle Zeit (17. – 19. Jh. n. Chr.)

4.4.1. Antoine Rossignol und die große Chiffre (17. Jh. n. Chr.)

Antoine Rossignol wurde 1600 in Frankreich geboren, wo die Fehde zwischen Katholiken und Protestanten noch immer andauerte. Zum ersten Mal trat er 1628 in Erscheinung, als Truppen von Heinrich II., Prinz von Condé, die Bastion Réalmont belagerten, wo sich die Verteidiger verschanzt hatten. Es gelang den Soldaten von Heinrich II. einen Boten von Réalmont gefangen zu nehmen und eine verschlüsselte Botschaft sicher zu stellen, aber nicht, diese auch zu entschlüsseln. Darum schickte Heinrich die Nachricht an Rossignol. Der entschlüsselte die Botschaft und fand heraus, dass die militärischen Vorräte der Belagerten gering waren. Die dechiffrierte Nachricht wurde den Truppen in Réalmont gezeigt. Mit ihrer Schwäche konfrontiert, ergaben sie sich sofort.
Einen weiteren wichtigen kryptoanalytischen Erfolg konnte Rossignol unter der Führung von Kardinal Richelieu feiern. Richelieu belagerte mit einer weiteren Armee die Festung La Rochelle. Auch dort gelang es den Männern Richelieus Briefe abzufangen, die Rossignol dann entschlüsselte. Aus den Briefen ging hervor, dass die Vorräte in der Festung zur Neige gingen und die Verteidiger auf Hilfe britischer Marinesoldaten warteten, die ihre Vorräte auffüllen sollten. Richelieu reagierte sofort. Als die Schiffe der britischen Armada kamen, wurde sie von Kanonen beschossen. Sie konnten den Hafen nicht anlaufen und mussten sich zurückziehen. Da die Vorräte in La Rochelle daraufhin ausgingen, mussten sich die Verteidiger ergeben.[123]
Antoine Rossignol wurde zum obersten Kryptologen ernannt. Er behielt seine Stellung auch unter Ludwig XIV. für den er, zusammen mit seinem Sohn Bonaventure, eine neue Verschlüsselung erfand, die „große Chiffre“. Die große

[122] Wrixon, Fred: Geheimsprachen, S. 30 ff.
[123] Wrixon, Fred: Geheimsprachen, S. 34 f.

Chiffre blieb über zwei Jahrhunderte unentschlüsselt, bis der französische Offizier Etienne Bazeries ihrer Entschlüsselung drei volle Jahre widmete. Er fand heraus, dass die große Chiffre mit 587 verschiedenen Zahlen zur Verschlüsselung arbeitete, dies ließ Bazeries zunächst glauben, dass sie Bigramme verschlüsselten, denn die Zahl möglicher Buchstabenpaare liegt mit $26^2 = 676$ sehr nahe. Doch damit hatte Bazeries keinen Erfolg. Die große Chiffre ersetzte nämlich keine Bigramme, sondern ganze Silben. Außerdem bauten die Rossignols einige Fallen in ihren Code ein, so standen einige Zahlen doch für einfache Buchstaben, Andere waren einfach als Füller angelegt und hatten überhaupt keine Bedeutung, wieder Andere löschten die vorangegangene Zahl.[124]

4.4.2. Napoléon Bonaparte (18. – 19. Jh. n. Chr.)

Napoléon Bonaparte wurde am 15. August 1769 auf Korsika geboren. Er arbeitete sich im Militär nach oben und war von 1799 bis 1804 erster Konsul der französischen Republik und anschließend bis 1815 Kaiser von Frankreich. Napoléon war ein hervorragender Stratege und Taktiker, doch sein heimliches Ass im Ärmel war die Tatsache, dass er eine Art Flaggensystem, den Signal-Telegrafen, verwendete. Als er seine Feldzüge durch Europa begann, ersetzte er dieses System allerdings durch geheimere Methoden der Kommunikation. Seine „petit chiffre“ war zwar nicht sichtbar, allerdings handelte es sich um ein sehr einfaches System mittels eines Nomenklators, der nur aus ca. zweihundert Symbolgruppen bestand. Die Simplizität dieses Systems hatte fatale Folgen für ihn. Die Russen hatten in der Kryptographie erhebliche Fortschritte gemacht und wahrscheinlich kein Problem damit gehabt die Nachrichten von Napoléon zu entschlüsseln, so wurde sein Russlandfeldzug vereitelt. Hinzu kam, dass das Feuer, welches sich um die Truppen ausbreitete, die Moskau belagerten, einige Abschriften seiner „petit chiffre“ zerstörten, sodass er einige Befehle in Klartext abfassen musste.
Die nächste große Niederlage erlitt Napoléon ein Jahr später vor Leipzig, wo er auf verbündete Truppen aus England, Belgien, Preußen und Österreich traf. Er hoffte auf einen geregelten Rückzug, doch seinem General Maréchal Augeraus unterlief ein

[124] http://www.cdc.informatik.tu-darmstadt.de/TI/Lehre/SS02/Seminar/Seminar_im_Grundstudium_PKI/Ausarbeitungen/PKI2002_Gruppe_2_Teil_1_Takac_Ausarbeitung/doc/PKI2002_Gruppe_2_Teil_1_Takac_Ausarbeitung-147.htm, letzter Zugriff: 23.03.2009.
http://www.ulm.ccc.de/old/chaos-seminar/krypto2/, letzter Zugriff: 23.03.2009.

Fehler bei der Verschlüsselung, sodass seine Nachricht von den Offizieren Napoléons unterschiedlich gedeutet wurde. Eigentlich sollten sie auf die Stadt vorrücken, die Hauptbrücke über der Elster einnehmen und Behelfsbrücken bauen, stattdessen rückten die Truppen nicht nur ohne Ordnung vor, sie sprengten darüber hinaus die Elsterbrücke auch noch. Napoléon und die Truppen, die ihm noch geblieben waren, mussten flüchten.[125]

4.5. Industriezeitalter (ab Mitte des 19. Jh. n. Chr.)

4.5.1. Samuel Morse (18. – 19. Jh. n. Chr.)

Samuel Morse wurde 1791 in Charlestown in den USA geboren. Morse war Kunstprofessor. Heute ist er allerdings für seine erfinderische Leistung viel bekannter, allen voran die des Schreibtelegrafen, oder zu seinen Ehren auch Morseapparat. Als er 1838 die erste telegrafische Nachricht versandte, läutete er damit das Maschinenzeitalter ein. Sein erster Telegraf bestand aus einer Staffelei an der am Rahmen ein Pendel mit einem Stift befestigt war. Darunter wurde ein aufgerollter Papierstreifen von einem Uhrwerk gezogen. Außerdem gehörte ein Elektromagnet zu seiner Erfindung. Der Stift zeichnete einen geraden durchgehenden Strich auf das Papier. Wenn allerdings ein Strom floss, so beeinflusste der Elektromagnet das Pendel und der Stift malte einen etwa v-förmigen Zacken. Später änderte Morse sein System so ab, dass der Stift das Papier nicht dauerhaft beschrieb, sondern nur dann, wenn der Strom floss. Abhängig von der Länge des Stromflusses entstanden auf dem Papier dann Linien oder Punkte. Doch erst fünf Jahre nach seiner Erfindung, im Jahre 1843, konnte er den Kongress davon überzeugen und es wurde eine 60km lange Telegrafenleitung von Washington D.C. nach Baltimore gebaut. Der Morsecode war ein Durchbruch, da man geheime Botschaften nun nicht mehr visuell übertragen musste, sondern sie binnen kürzester Zeit kilometerweit über Leitungen übertragen konnte. Jahrzehnte später fand Morses Mitarbeiter Alfred Vail heraus, dass die Zeichen nicht unbedingt auf Papier festgehalten werden mussten, sondern auch akustisch dargestellt und entziffert werden konnten. Das hatte einerseits den Vorteil, dass einem Angreifer keine Schriftstücke in die Hände fallen konnten, die dieser dann entschlüsseln konnte,

[125] Wrixon, Fred: Geheimsprachen, S. 50 f.
http://de.wikipedia.org/wiki/Napoléon_Bonaparte, letzter Zugriff: 23.03.2009.

andererseits hatte es Nachteile, wenn man Teile der Botschaft nicht verstanden hatte.[126]

4.5.2. Playfair-Chiffre (19. Jh. n. Chr.)

Die Playfair-Chiffre wurde von Sir Charles Wheatstone als Verschlüsselungsmethode für die Telegrafie entwickelt. Lord Lyon Playfair war ein enger Freund von Wheatstone und führte die Chiffre dem Innenminister, sowie Prinz Albert vor. Er empfahl diese Methode für den militärischen Gebrauch. Da Playfair bekannt war und diese Chiffre so intensiv bewarb, wurde sie schnell mit seinem Namen in Verbindung gebracht, weshalb sie Playfair-Chiffre heißt und nicht nach dem Entwickler Wheatstone benannt ist. Die Chiffre selbst unterscheidet sich von anderen Verfahren in erster Linie dadurch, dass sie keine Einzelzeichen verschlüsselt, sondern Bigramme.[127]

4.5.3. Charles Babbage (19. Jh. n. Chr.)

Charles Babbage könnte man fast als einen Universalgelehrten der Neuzeit bezeichnen. Er wurde 1791 in Walworth in England geboren und war Mathematiker, Philosoph, Erfinder und Ökonom. Heutzutage würde man ihn wohl auch noch Informatiker nennen. Er entwickelte zwei mechanische Rechenmaschinen, die „difference engine“ und die „analytical engine“. Die zweite gilt heute als ein Vorläufer des modernen Computers. Obwohl er einen überragenden Durchbruch in der Kryptoanalyse feierte, wurde er dafür erst posthum berühmt, weil er sein Werk nie veröffentlichte. Charles Babbage war es im Jahre 1854, als erster Person überhaupt, gelungen die polyalphabetische Vigenère-Chiffre zu knacken, die lange Zeit als unknackbar galt. Seine Abhandlung dazu wurde erst nach seinem Tod von Wissenschaftlern entdeckt. Warum er es geheim hielt ist unbekannt. Offensichtlich hatte Babbage wohl grundsätzlich die Angewohnheit seine Entdeckungen unveröffentlicht zu lassen, doch für den Bruch der Vigenère-Chiffre gibt es auch eine andere Theorie: Es könnte der britische Geheimdienst gewesen sein, der Babbage

[126] Wrixon, Fred: Geheimsprachen, S. 52.
http://de.wikipedia.org/wiki/Samuel_Morse, letzter Zugriff: 24.03.2009.
[127] Wrixon, Fred: Geheimsprachen, S. 52 ff.
http://de.wikipedia.org/wiki/Playfair, letzter Zugriff: 24.03.2009.

zwang seine Arbeit geheim zu halten um sich damit einen Vorteil im Krimkrieg zu sichern, der kurz zuvor ausgebrochen war.[128]

4.5.4. Friedrich Kasiski (19. Jh. n. Chr.)

Zeitgleich mit Babbage lebte der, 1805 in Preußen geborene, Infanteriemajor Friedrich Wilhelm Kasiski. Im Jahre 1863 veröffentlichte er sein Buch „Die Geheimschriften und die Dechiffrierkunst“, das ihn in kryptologischen Kreisen berühmt machte. Kasiski war es neun Jahre nach Babbage gelungen die Vigenère-Chiffre zu knacken, doch da Babbage sein Werk nicht veröffentlicht hatte, galt er zu jener Zeit als der Erste, dem das gelungen war. Kasiski beschreibt in seinem Buch ein Verfahren die Länge eines Schlüsselwortes zu ermitteln, das für die Vigenère-Verschlüsselung verwendet wurde. Das Verfahren wird noch heute als Kasiski-Test bezeichnet.[129]

4.5.5. Auguste Kerckhoffs (19. Jh. v. Chr.)

Auguste Kerckhoffs hieß mit vollem Namen Jean-Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwendhof. Er wurde 1835 in Nuth in den Niederlanden geboren und galt als herausragender Kryptologe. Sein Hauptwerk war „la Cryptographie militaire“, welches er 1883 veröffentlichte. Darin unterscheidet Kerckhoffs als erster Kryptologe zwischen dem Verfahren und dem Schlüssel und erklärt, dass die Sicherheit eines Verfahrens nicht von der Geheimhaltung des Verfahrens abhängen dürfe, sondern von der Sicherheit des Schlüssels abhängen müsse, sodass eine Geheimschrift nicht geknackt werden kann, wenn das Verfahren bekannt ist. Dieser Grundsatz wurde als „Kerckhoffs Prinzip“ oder „Kerckhoffs Maxime“ bekannt und ist noch heute in der Kryptographie gültig.[130]

---

[128] Singh, Simon: Geheime Botschaften, S. 104.
http://de.wikipedia.org/wiki/Babbage, letzter Zugriff: 24.03.2009.
[129] Singh, Simon: Geheime Botschaften, S. 103 f.
http://de.wikipedia.org/wiki/Kasiski, letzter Zugriff: 24. 03.2009.
[130] Wrixon, Fred: Geheimsprachen, S. 605 f.

4.6. Der Erste Weltkrieg

Wie in vielen anderen Kriegen auch, spielte die Kryptologie eine zentrale Rolle im Ersten Weltkrieg. Zu den wohl herausragendsten Leistungen dieses dunklen Kapitels zählt die Entschlüsselung der ADFGVX-Chiffre.

4.6.1. Painvin und ADFGVX

Georges Jean Painvin wurde 1886 in Nantes geboren. Er war Geologe und erfolgreicher Unternehmer. Er war Manager der größten französischen Chemiekonzerne. Doch er selbst betrachtete seinen Lebtag lang die Entschlüsselung der ADFGX bzw. ADFGVX-Chiffre der deutschen im ersten Weltkrieg als die größte Leistung seines Lebens. Im März 1918 planten die Deutschen eine Großoffensive gegen Frankreich. Um die Pläne dafür geheim zu halten, hatten sie ihre Chiffriermethode verändert. Die französische Aufklärung fing plötzlich nur noch Funksprüche ab, die die fünf Zeichen A, D, F, G und X enthielten. Wegen der Umstellung rechneten sie tatsächlich mit einem Angriff, weshalb die Entschlüsselung der neuen ADFGX-Chiffre für sie von größter Bedeutung war. Die Aufklärung kam schnell zu dem Ergebnis, dass die Buchstaben gewählt wurden, weil sie sich im Morsealphabet stark unterschieden und somit Übertragungsfehler vermieden werden konnten, doch sie konnten die Chiffre nicht brechen. Painvin opferte der Methode drei Monate, in denen er Tag und Nacht daran arbeitete. Kryptographiehistoriker sagen außerdem, dass er in dieser Zeit deutlich an Gewicht verlor, wobei die Zahlen zwischen 15 und 33 Pfund schwanken. Die Deutschen waren währenddessen auf dem Vormarsch und als sie kurz vor Paris standen, war es Painvin endlich gelungen die Chiffre zu knacken. Doch die Freude währte nicht lange, kaum hatte Painvin die Chiffre geknackt und die Franzosen damit in die Lage versetzt den deutschen Funkverkehr zu überwachen, schon hatten die Deutschen erneut ihre Methode geändert. Nun tauchte in den deutschen Nachrichten neben den fünf bekannten Buchstaben auch noch das „v“ auf. Doch da es sich bei dem neuen Verfahren nur um eine Abwandlung des Alten handelte, brauchte Painvin nicht lange, um sie zu entschlüsseln. Am 1. Juni 1918 fingen die Aufklärer die erste Nachricht ab, die mit der neuen ADFGVX-Methode verschlüsselt worden war. Nachdem Painvin für das Original-Verfahren drei Monate benötigt hatte, reichten ihm diesmal etwas mehr als

24 Stunden aus. Am Abend des 2. Juni hatte er die Chiffre bereits gebrochen. Die Offensive der Deutschen auf Paris konnte abgewehrt und sie konnten in der Folgezeit zurückgedrängt werden.[131]

4.7. Der Zweite Weltkrieg (1939 – 1945)

Am 1.9.1939 griff Deutschland Polen ohne vorherige Kriegserklärung an. Dieses Datum gilt als offizieller Beginn des Zweiten Weltkrieges. Während in den meisten Kriegen seit der Antike Geheimschriften eine wichtige Rolle spielten, stand die Kryptographie im Zweiten Weltkrieg im zentralen Mittelpunkt des Geschehens, als die Alliierten Jagd auf die deutsche Verschlüsselungsmaschine Enigma machten.

4.7.1. Die Enigma

Kein anderes kryptographisches Verfahren in der Geschichte hat ein ähnliches Aufsehen (auch bei der laienhaften Bevölkerung) erregt wie die Verschlüsselungsmaschine der Deutschen im Zweiten Weltkrieg, die Enigma. Ein Beleg dafür sind die unzähligen Bücher, die sich mit der Maschine befassen. Geschichten über die Enigma oder der Versuch der Alliierten an sie heranzukommen wurden sogar mehrfach verfilmt. Das Wort „Enigma“ ist griechischen Ursprungs und bedeutet „Rätsel“.

Die Deutschen hatten einen kryptographischen Schock erlitten, nachdem Winston Churchill 1923 sein Buch „The world crisis“ veröffentlichte, in dem er beschrieb, wie die Briten die Codebücher der Deutschen erringen und damit einen Großteil des deutschen Marinefunks im Ersten Weltkrieg entschlüsseln konnten. In dieser Phase wandte sich Arthur Scherbius an die deutsche Regierung, der 1918 eine Chiffriermaschine entwickelt hatte, die auf einem Rotorensystem basierte mit der eine immense Anzahl an Geheimtextalphabeten erzeugt werden konnte. Die Deutschen erkannten das Potential der Maschine und 1926 wurde die erste Enigma bei der deutschen Armee in den militärischen Betrieb genommen. In den folgenden beiden Jahrzehnten kaufte das deutsche Militär 30.000 solcher Maschinen. Fast

[131] Wrixon, Fred: Geheimsprachen, S. 74 f.
Singh, Simon: Geheime Botschaften, S. 132 ff.
Kippenhan, Rudolf: Verschlüsselte Botschaften, S. 190 ff.
http://de.wikipedia.org/wiki/Painvin, letzter Zugriff: 25.03.2009.

zeitgleich zu Scherbius und unabhängig voneinander, hatten drei weitere Erfinder sehr ähnliche Ideen einer rotorgestützten Chiffriermaschine: bereits ein Jahr vor Scherbius, der Amerikaner Edward Hebern. Sein Verhängnis war, dass seine Erfindung in die Zeit der Saubermann-Politik von Hoover fiel, sodass er seine Maschine nicht durchsetzen konnte. Außerdem ein Jahr nach Scherbius der Niederländer Hugo Koch und der Schwede Arvid Damm, doch auch ihnen gelang es nicht ihre Erfindung an den Mann zu bringen. Scherbius hingegen verkaufte seine Maschine nicht nur an das deutsche Militär, sondern auch an Firmen, allerdings verdrahtete er die Maschinen unterschiedlich, sodass aus den, in Firmen kommerziell genutzten, Maschinen nur wenige Rückschlüsse für die mit der militärischen Variante durchgeführte Verschlüsselung gewonnen werden konnte.
Außerdem setzten die Deutschen verschiedene Versionen der Enigma für ihre unterschiedlichen Truppenverbände, also Luftwaffe, Heer und Marine, ein. Die Aufgabe Enigma zu knacken schien nahezu unmöglich, doch die Alliierten, allen voran die Briten, setzten ihre Kryptoanalytiker dagegen.[132]

4.7.2. Ultra und der Kampf gegen die Enigma

Winston Churchill war sieben Monate nach Beginn des Zweiten Weltkrieges Premierminister von Großbritannien geworden. Aus den Erfahrungen des ersten Weltkrieges hatte er gelernt, wie wichtig der Informationsfluss mittels Funkaufklärung war. Daher unterstützte er unterschiedliche Geheimdienste. Eine von diesen Kryptoanalyseabteilungen war die „Government Code and Cypher School“ in Bletchley Park unweit von London. Das riesige, fast aussichtslos erscheinende, Projekt „Entschlüsselung der Enigma“ erhielt den Codenamen Ultra und war eines der bestgehüteten Geheimnisse der Militärgeschichte, da man auf jeden Fall verhindern wollte, dass die Deutschen Notiz davon nahmen.
1929 wurde eine Enigma-Version fälschlicherweise nach Warschau geliefert. Geheimagenten hatten Fotos und Diagramme dieser Maschine angefertigt. Gemeinsam mit einigen kommerziell vertriebenen Varianten, gelang es Forschern von der Universität Posen grundlegende mathematische Probleme bei der Verschlüsselung der Enigma zu lösen. Seit Oktober 1931 verkaufte ein Angestellter des deutschen Verteidigungsministeriums, Hans-Thilo Schmidt, der im Ersten

[132] Wrixon, Fred: Geheimsprachen, S. 82 f.
Singh, Simon: Geheime Botschaften, S. 172 ff.

Weltkrieg gedient hatte, jedoch Opfer der Kürzungen durch den Versailler Vertrag wurde und daher von Deutschland enttäuscht war, Geheimakten, darunter eine Gebrauchsanweisung einer militärischen Enigma, ein Codebuch mit Schlüsseln, Verschlüsselte Botschaften mitsamt ihrem zugehörigen Klartext und Anleitungen zur Modifizierung der Maschine, an die Franzosen. Frankreich kam sehr schnell dahinter, dass die Enigma der Maxime von Kerckhoffs folgte, die ja gerade besagt, dass die Sicherheit einer Verschlüsselung von dem Schlüssel und nicht von dem Verfahren abhängt. In dem Glauben, dass es unmöglich sei den passenden Schlüssel herauszufinden, bauten sie mit den ihnen zur Verfügung stehenden Unterlagen nicht einmal eine Kopie des Geräts. Allerdings hatten sie ein Abkommen mit Polen, denen sie die Pläne überließen.

4.7.3. Marian Rejewski

In Polen arbeitete der begnadete Kryptoanalytiker Marian Rejewski in der Dechiffrierabteilung Biuro Szyfrów. Er analysierte die Pläne der Enigma genauestens. Und darüber hinaus die, von der Enigma überschlüsselten Codes, die die Deutschen zu Beginn einer Nachricht mit sandten. Schließlich gelang es ihm die einzelnen Buchstaben miteinander in Beziehung zu setzen. Rejewski entwickelte daraufhin eine Maschine, die automatisch nach den richtigen Walzenstellungen suchte. Sechs solcher Maschinen arbeiteten parallel in einer Anlage, die den Namen „bomba“ bekam. Rejewskis Bomben konnten die jeweiligen Enigma-Schlüssel in ca. zwei Stunden herausfinden und waren das erste mechanische Kryptoanalysegerät. Rejewskis Erfolg in der Enigma-Entschlüsselung war 1932, also 7 Jahre vor dem Zweiten Weltkrieg. 1938, ein Jahr vor Kriegsbeginn erweiterten die Deutschen die Enigma um zwei Walzen. Das reichte aus um Rejewski vollends zu überfordern. Anstelle der sechs Bomben, welche die deutschen Codes bislang ermittelt hatten, benötigte er nun 60 solcher Bomben. Dafür fehlten der Abteilung, für die er arbeitete aber die finanziellen Mittel. Wieder einmal schien die deutsche Enigma nicht zu knacken. Daraufhin kam es zu einem Treffen polnischer, französischer und britischer Kryptologen, bei dem die Polen ihre Nachbauten und deren Methoden weitergaben.[133]

[133] Wrixon, Fred: Geheimsprachen, S. 83 f.
Singh, Simon: Geheime Botschaften, S. 179 ff.
http://de.wikipedia.org/wiki/Enigma_(Maschine), letzter Zugriff: 25.03.2009.

4.7.4. Alan Turing

Die Briten machten sich die Vorarbeit der Polen zunutze. Bletchley Park bot genügend Menschen Platz, die sich mit der Kryptoanalyse befassen konnten, außerdem stand der dortigen Abteilung ein deutlich höheres Budget zur Verfügung, sodass die nötigen Bomben angeschafft werden konnten. Allerdings wurde die Enigma immer wieder verändert, was die Kryptoanalytiker zwang auch ihre Bomben umzubauen.

Alan Turing war einer der Kryptoanalytiker in Bletchley Park. Er wurde 1912 in London geboren. 1931 ging er ans King's College in Cambridge und legte eine steile Karriere hin. Während er dort studierte und später arbeitete entwarf er die Turing-Maschine, einen Vorläufer des modernen Computers, außerdem legte er theoretische Grundlagen des Computers. 1939 wurde er von Bletchley Park abgeworben, wo er sich mit der Enigma und ihrer Entschlüsselung beschäftigte. Turing konzentrierte sich bei seiner Suche auf sogenannte Cribs, Anhaltspunkte, die er aus den Gewohnheiten der Deutschen gewann, so wurde beispielsweise jeden morgen gegen sechs Uhr der Wetterbericht verschlüsselt übertragen. Aus den klaren Strukturen der deutschen Nachrichtenübermittlung konnte Turing ohne Entschlüsselung abschätzen an welcher Stelle in diesem Bericht etwa das Wort Wetter auftauchte. Wenn er das verschlüsselte Wort Wetter gefunden hatte und wusste, dass es auch Wetter bedeuten sollte, so war Turing klar, dass er diesen Crib nutzen konnte, um die Walzen so zu konfigurieren, dass aus dem Wort Wetter das verschlüsselte Wort, welches er vor sich hatte, entstand. Das Problem dabei war nur die unzählige Anzahl verschiedener Walzeneinstellungen die man durchprüfen musste. Turing entwickelte daraufhin eine eigene Bombe die bedeutend größer war als die von Rejewski, allerdings nicht mehr die sechs Zeichen zu Beginn der Nachricht unter die Lupe nahm, sondern gezielt die Cribs studierte um dann die entsprechenden Walzenkonfigurationen zu testen. 1940 gelangen den Briten die ersten Entschlüsselungen der Enigma. In der Folgezeit wurden die Bomben erweitert und immer effektiver. Einige Historiker glauben heute, dass die Entschlüsselung der Enigma etwa ein Jahr Krieg ersparte.[134]

[134] Singh, Simon: Geheime Botschaften, S. 205 ff.
Kippenhahn, Rudolf: Verschlüsselte Botschaften, S. 232 ff.
http://de.wikipedia.org/wiki/Alan_Turing, letzter Zugriff: 25.03.2009.

4.7.5. Colossus und Mark II

Die militärische Kryptographie wurde im Zweiten Weltkrieg von Maschinen beherrscht. Das führte dazu, dass auch die Kryptoanalytiker oftmals auf Maschinen zurückgreifen mussten um die immense Anzahl an verschiedenen Möglichkeiten in einem sinnvollen Zeitrahmen durchprobieren zu können, wie z.B. die Bomben von Rejewski und Turing. Eine dieser Maschinen trug den Namen Colossus, ihr Nachfolger hieß Mark II. Der Colossus wurde im Dezember 1943 in Bletchley Park aufgestellt und konnte die Chiffren des „Geheimschreibers“, auch Lorenz-Schlüsselmaschine genannt, brechen. Das System der Lorenz-Schlüsselmaschine, war, wegen eines Fehlers bei der Einführung, bereits 1942 durchschaut, allerdings musste man zu jeder Nachricht die ursprüngliche Stellung der Räder ermitteln, dies konnte mehrere Tage dauern. Der Colossus, der auf den Ideen einer universellen Maschine von Alan Turing aufgebaut war, schaffte hingegen mehrere Tausend Kombinationen binnen Sekunden zu überprüfen, sodass sie eine Lorenz-Schrift innerhalb weniger Stunden knacken konnte.[135]

4.7.6. Der Navajo-Code

Obwohl die Maschinen die Kryptographie im Zweiten Weltkrieg beherrschten, waren nicht alle Geheimcodes Maschinenchiffren, denn die Maschinenverschlüsselung hatte einen großen Nachteil, sie erforderte Platz für die Maschinen selbst und war zeitaufwendig. Dies stellte zwar für die Funkaufklärungsbüros auf dem Festland und auf Kriegsschiffen kein Problem dar, doch sehr wohl an den direkten Kampfschauplätzen an der Kriegsfront. In der Hektik des Gefechts mussten schnelle taktische Bewegungen im Klartext übermittelt werden, was zu enormen Sicherheitsrisiken führte. Philip Johnston war Ingenieur Los Angeles und hatte eine Idee, wie man dieses Problem beheben könnte. Er hatte in seiner Kindheit in einem Navajo-Reservat gelebt und sprach die Sprache der Ureinwohner fließend. Er schlug vor, dass man die Truppen mit ihnen als Funker ausstatten sollte. Nach einer argwöhnischen Beäugung wurde die Idee auf die Probe gestellt und als sinnvoll umsetzbar betrachtet. Die Wahl, welcher Stamm der Ureinwohner nun tatsächlich die

[135] Wrixon, Fred: Geheimsprachen, S. 103.
http://de.wikipedia.org/wiki/Colossus, letzter Zugriff: 26.03.2009.

Funker stellen sollte, fiel schließlich auf die Navajo-Indianer, weil Johnston einwenden konnte, dass sie der einzige Stamm waren, der zuvor nicht von deutschen Gelehrten untersucht wurde und demnach kaum jemand der Sprache der Navajo mächtig sei. Der Navajo-Code war ein voller Erfolg und brachte den U.S. Streitkräften entscheidende Vorteile.[136]

4.8. Die moderne Kryptologie

4.8.1. DES und AES

Im Zuge der Mechanisierung der fünfziger und sechziger Jahre musste eine Verschlüsselung für zivile Zwecke gefunden werden. Das „National Bureau of Standarts“ (NBS) suchte nach einem Verfahren das Kerckhoffs‘ Prinzip zugrunde legte. Das Verfahren musste öffentlich bekannt sein und die Sicherheit ausschließlich vom verwendeten Schlüssel abhängen. Die Computerfirma International Business Machines (IBM) nahm sich diesem Unterfangen an und 1976 wurde der „Data Encryption Standard“ (DES) vorgestellt. Der DES ist eine Blockchiffre, in 16 Runden werden die Blöcke Substitutionen und Transpositionen unterzogen. Zunächst sollten 64 Binärzahlen zur Darstellung des Klartextes verwendet werden, die NSA konnte IBM aber davon überzeugen, dass 56 ausreichen würden, was zu Spekulationen über die Sicherheit des DES führte. Viele glaubten, dass die NSA sich eine Hintertür eingebaut habe, um den relativ sicheren DES bei Bedarf schnell aushebeln zu können. Eine solche Hintertür wurde jedoch nie gefunden. Allerdings sind die 56 Bit der Grund dafür, weshalb der ursprüngliche DES heute kaum noch Verwendung findet, da er für die Kapazitäten heutiger Computer als zu schwach gilt.[137]
Im Oktober 2000 trat sein Nachfolger auf den Plan, der „Advanced Encryption Standart“ (AES) von Joan Daemen und Vincent Rijmen. Der AES hat den Vorteil, dass die Größe der Blöcke auf 128 Bit angehoben wurde, die Länge des verwendeten Schlüssels ist hingegen Variabel und kann 128, 192 oder 256 Bit betragen.[138]

---

[136] Singh, Simon: Geheime Botschaften, S. 236 ff.
[137] Wrixon, Fred: Geheimsprachen, S. 126 f.
http://de.wikipedia.org/wiki/Data_Encryption_Standard, letzter Zugriff: 26.03.2009.
[138] http://de.wikipedia.org/wiki/Advanced_Encryption_Standard, letzter Zugriff: 26.03.2009.

4.8.2. Public Key

Der Begriff „Public Key“ (zu Deutsch: „öffentlicher Schlüssel“) ist untrennbar mit drei Namen der Kryptologie verbunden: Martin Hellman, Whitfield Diffie und Ralph Merkle. Martin Hellman wurde 1945 in New York geboren und wurde 1971 Professor an der Universität Stanford. Dort widmete er sich dem kryptologischen Problem der Schlüsselübertragung. Der Schlüsselübertrag ist nicht nur irgendein Problem, es ist das zentrale Problem der Kryptographie. Will man eine geheime Nachricht austauschen, so muss man sie verschlüsseln, wenn man das getan hat, muss man aber diesen Schlüssel übertragen und der Schlüssel muss ebenfalls geheim bleiben, denn wer den Schlüssel hat, kann auch die Nachricht entziffern. Man muss also, um ein Geheimnis zu übertragen, bereits im Vorfeld ein Geheimnis übertragen haben. Simon Singh bezeichnet diesen Umstand in seinem Buch als die „klassische Paradoxie“[139]. 1969 war der erste Vorläufer des heutigen Internet entstanden, das ARPAnet. Whitfield Diffie erkannte schon damals, welche Möglichkeiten die Vernetzung mit sich brachte und glaubte, dass auch Privatpersonen eines Tages dieses Medium massiv nutzen würden. Doch er erkannte auch die Probleme, die das mit sich bringen würde. Zur Wahrung der Privatsphäre musste eine Möglichkeit gefunden werden, wie die Schlüssel zwischen zwei Fremden, die sich gerade erst kennengelernt hatten, ausgetauscht werden konnten. Das brachte ihn dazu sich ab Anfang der 70er Jahre mit dem Problem der Schlüsselübertragung zu beschäftigen. 1974 erfuhr er von Martin Hellman, der sich mit der gleichen Problematik auseinander setzte. Er traf sich mit Hellman und beide wurden zu Partnern. Wenig später bereicherte Ralph Merkle das kleine Team. Bevor Merkle sich den beiden anschloss, hatte er als Student bereits eine mögliche Lösung gefunden, doch er konnte seinen Professor nicht von seiner Methode überzeugen, da dieser kein Verständnis dafür aufbrachte, wie sich jemand mit dem Problem des Schlüsselübertrags beschäftigen konnte. Bis zu diesem Zeitpunkt war die einhellige Meinung in der Wissenschaft gewesen, dass es keine andere Lösung geben könne, als den Schlüssel über irgendeinen mehr oder weniger unsicheren Übertragungsweg zu verschicken. 1976 gelang ihnen der Durchbruch, als sie ihre Forschungsarbeit „New Directions in Cryptography“ (Deutsch: „Neue Wege in der Kryptographie“) veröffentlichten. Hellman hatte mit Hilfe der modularen Arithmetik einen Weg

[139] Singh, Simon: Geheime Botschaften, S. 311.

gefunden, wie zwei Personen sich über Einwegfunktionen einen gemeinsamen Schlüssel generieren konnten, ohne den endgültigen Schlüssel übertragen zu müssen.
Während Hellman an einem Weg arbeitete den Schlüssel sicher zu übertragen, kam Diffie auf eine andere bahnbrechende Idee: Vielleicht musste der Schlüssel überhaupt nicht übertragen werden. Sämtliche Verfahren der Kryptographiegeschichte verwendeten einen Schlüssel, um einen Klartext zu verschlüsseln und sie verwendeten den gleichen Schlüssel, um ihn wieder zu entschlüsseln. Diffie hatte den Einfall gehabt ein Schlüsselpaar zu erzeugen, also zwei unterschiedliche Schlüssel von denen einer ausschließlich der Verschlüsselung diente und der andere der Entschlüsselung. Bei einem solchen Verfahren fiele die Übertragung der Schlüssel weg, weil dem Absender der Nachricht die Kenntnis über den Schlüssel zur Verschlüsselung genügt und der Empfänger den Gegenschlüssel geheim halten kann. Diffie glaubte, dass sich ein solches Schlüsselpaar über mathematische Einwegfunktionen generieren lassen könnte. Diffie, Hellman und Merkle waren Visionäre auf ihrem Gebiet, doch es gelang ihnen nicht eine Funktion zu finden, die Diffies Idee praktisch umsetzen konnte.[140]

4.8.3. Das RSA-Verfahren

Dieses Meisterstück gelang einem Trio bestehend aus Ron Rivest, Adi Shamir und Leonard Adleman. Die Anfangsbuchstaben ihrer Nachnamen liefern den Namen für das Verfahren. Rivest und Adleman lehrten und forschten am Massachusetts Institute of Technology. Adi Shamir hatte gerade seinen Doktortitel errungen und kam zu Forschungszwecken dorthin, wo er sich dem Team anschloss. Rivest war die Arbeit von Diffie, Hellman und Merkle in die Hände gefallen und er verbiss sich in die Vorstellung, dass es eine Einwegfunktion geben müsse, die Diffies Idee einer asymmetrischen Verschlüsselung umsetzen könne. Im April 1977 fand Rivest in einer schlaflosen Nacht die Lösung. Leonard Adleman, der in dem Team die Aufgabe hatte die Ideen Rivests und Shamirs auf Herz und Nieren zu prüfen, was meistens mit dem Ergebnis endete, dass er sie zerlegte und für nicht verwendbar einstufte, weil sie irgendwo eine Schwachstelle aufwiesen, konnte eben jenen Nachteil in der neuen

[140] Wrixon, Fred: Geheimsprachen, S. 127 f.
Singh, Simon: Geheime Botschaften, S. 306 ff.
Schmeh, Klaus: Kryptographie, S. 674 ff.

Idee Rivests nicht mehr finden. Das RSA-Verfahren war geboren. Der RSA-Algorithmus gilt zwar als theoretisch angreifbar, als praktisch jedoch nicht, da er sich bei der Erzeugung des Schlüsselpaares auf das Produkt aus sehr großen Primzahlen stützt. Je größer die Primzahlen sind, desto sicherer ist das Verfahren. Eine Hochrechnung hat ergeben, dass für Primzahlen im Bereich von 10^{308} hundert Millionen PCs über tausend Jahre für die Primfaktorzerlegung benötigen würden. Damit gilt das Verfahren in der Praxis als sicher.[141]

4.8.4. International Data Encryption Algorithm(IDEA)

Der International Data Encryption Algorithm (IDEA) wurde von James Massey und Xueija Lei entwickelt. IDEA sollte eine Alternative zu dem, zu diesem Zeitpunkt üblichen, DES-Verfahren darstellen. IDEA ist eine Blockchiffre und arbeitet ähnlich wie DES, allerdings konnte IDEA eine größere Schlüssellänge (128 Bit) aufweisen, dafür beschränkt sich das Verfahren auf die Hälfte an Durchlaufrunden. Die dabei durchgeführten Anwendungen unterscheiden sich allerdings von DES. IDEA setzte auf Operationen der modularen Mathematik mit der die 64-bit Blöcke verwürfelt wurden. Da IDEA keine Sicherheitslücken aufwies und mit der größeren Schlüssellänge punkten konnte, machte es seiner Aufgabe als DES-Alternative alle Ehre. Einen weiteren Aufschwung erhielt das Programm, als es von Phil Zimmermann in seinem Programm „Pretty Good Privacy“ (PGP) eingesetzt wurde. Als der DES-Nachfolger AES auf die Bildfläche trat, verlor IDEA allerdings an Beachtung.[142]

4.8.5. Pretty Good Privacy (PGP)

1989 wurde im Forschungszentrum CERN das World Wide Web entwickelt. 1993 wurde es weltweit zugänglich gemacht und die Erfolgsgeschichte nahm ihren Lauf. Das Internet wird heute von ca. 1,2 Mrd. Menschen genutzt, das entspricht ca. 20% der Weltbevölkerung.[143] Die Verwendung erstreckt sich dabei vom Ansehen einfacher Inhalte bis hin zur Übermittlung streng vertraulicher Daten, wie etwa

[141] Wrixon, Fred: Geheimsprachen, S. 127 f.
Singh, Simon: Geheime Botschaften, S. 329 ff.
[142] Schmeh, Klaus: Kryptographie, S. 146 f.
[143] http://www.bitkom.org/46074_46069.aspx, letzter Zugriff: 27.03.2009.

Banktransaktionen oder Einkäufe. Whitfield Diffie hatte mit seiner Vorausahnung Anfang der 70er Jahre also recht gehabt. Die massive Informationsflut war jedoch anfangs nicht sicher gewesen, bis Phil Zimmermann auf den Plan trat. Zimmermann vertrat die Auffassung, dass der Mensch in seinem Recht auf Privatsphäre und Sicherheit auch im globalen Internet nicht eingeschränkt werden dürfe, also verfolgte er das Ziel, die Kryptographie auch dem privaten Nutzer zugänglich zu machen. Er entwarf das Programm „Pretty Good Privacy“ (PGP) womit er in harsche Kritik geriet. Die Behörden hatten die Bedenken, dass ein öffentliches Kryptographiesystem auch von Kriminellen genutzt würde, um ihre Machenschaften vor den Fahndern zu verheimlichen. Dennoch blieb Zimmermann bei seiner Auffassung, der Mensch müsse sich auch im Informationszeitalter seiner Persönlichkeitsrechte sicher sein dürfen. Auch ein gerichtliches Untersuchungsverfahren ließ ihn nicht von seinem Weg abkommen. PGP verwendet eine hybride Verschlüsselung. Die ersten Versionen stützten sich auf das RSA-Verfahren, doch Zimmermann fand schnell heraus, dass das RSA-Verfahren zwar sicher, aber auch sehr rechenintensiv war, also verwendete er in späteren Versionen relativ sichere symmetrische Verfahren, wie z.B. IDEA, und wand den RSA-Algorithmus auf die Schlüssel an. Die Exportgesetze der USA sahen aber damals vor, dass kryptographische Programme mit einer Schlüssellänge von über 40 Bit unter spezielle Richtlinien des Exportgesetzes fielen. Die von Zimmermann verwendeten IDEA-Versionen hatten aber eine Schlüssellänge von 128 Bit und die USA verhängten eine Sperre für den lizenzfreien Export von PGP. Der Idealist Zimmermann schrieb daraufhin sein Programm in einem Buch nieder und exportierte dieses. Über 60 Freiwillige tippten den Programmcode ab und entwickelten eine internationale Version von PGP.[144]

5. Kryptographie

5.1. Klassische kryptographische Verfahren

Die klassischen kryptographischen Verfahren habe ich nach ihrer Methode in Transpositionen, monoalphabetische Substitutionen und polyalphabetische Substitutionen unterteilt.

[144] Wrixon, Fred: Geheimsprachen, S. 129.
Singh, Simon: Geheime Botschaften, S. 353 ff.
http://de.wikipedia.org/wiki/Pretty_Good_Privacy, letzter Zugriff: 27.03.2009.

5.1.1. Transpositionschiffren

5.1.1.1. Spaltentransposition[145]

Eine der einfachsten Formen der Transpositionsalgorithmen ist sicherlich die Spaltentransposition. Dabei wird der Text einfach zeilenweise in eine Matrix geschrieben und anschließend spaltenweise ausgelesen.
Betrachten wir das folgende Beispiel. Der Begriff „Kryptologie“ wird zunächst in eine Tabelle mit drei Zeilen und vier Spalten geschrieben.

K	R	Y	P
T	O	L	O
G	I	E	

Abbildung 4.1

Liest man nun Spalte für Spalte erhält man den Geheimtext „KTGROIYLEPO“. Die Spaltentransposition lässt einige Variationsmöglichkeiten zu, so könnte man die Spalten nach gewissen Vorgaben auslesen, z.B. in der Form 2-3-1-4. Dann würde der Text „ROIYLEKTGPO“ lauten. Denkbar wäre auch, dass man die Spalten von unten nach oben ausliest, oder im Wechsel, einmal von oben nach unten und anschließend von unten nach oben. An der Sicherheit des Verfahrens ändert sich dabei allerdings nicht allzu viel, zumal der Empfänger der Nachricht über solche Variationen in Kenntnis gesetzt werden muss.

5.1.1.2. Skytale von Sparta[146]

Eine Transpositionschiffre, die der Spaltentransposition sehr ähnlich ist, verwendeten bereits die Spartaner um etwa 500 v. Chr.: Die Skytale von Sparta. Die Spartaner verwendeten dazu einen Holzstock, um den sie ein Lederband wickelten. Die Nachricht wurde dann der Länge nach von links nach rechts auf das Lederband geschrieben, wobei auf jeden Abschnitt des Bandes immer nur ein Buchstabe geschrieben wird. Wickelte man es ab, so erhielt man automatisch die Reihenfolge der Buchstaben von oben nach unten gelesen.

[145] Wätjen, Dietmar: Kryptographie, S. 13.
[146] Beutelspacher, Albrecht: Kryptologie, S. 3 f.

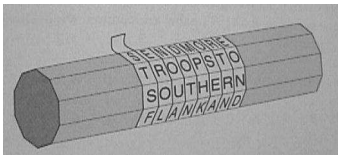


Abbildung 4.2

Geht man in obigem Beispiel davon aus, dass die nicht sichtbaren Seiten auch nicht beschrieben sind (was zwar unrealistisch ist, aber an dieser Stelle keine Rolle spielt), dann würde man nach abrollen des Bandes folgenden Text lesen können: „STSFEROLNOUADOTNMPHKOSEARTRNEOND“. Die Abbildung zeigt sehr deutlich wie ähnlich sich Skytale und Spaltentransposition wirklich sind. Sowohl Skytale, als auch Spaltentransposition hängen von der Wahl des Holzstockes, bzw. der Größe der Matrix ab. Wählt man als Skytale ein Holzstück mit größerem oder kleinerem Umfang, so ergeben sich andere verschlüsselte Texte.

5.1.1.3. Gartenzaun-Transposition[147]

Ein anderes, allerdings wiederum recht ähnliches, Transpositionsverfahren ist die Gartenzaun-Transposition. Ihr Name leitet sich von dem Aussehen der Matrix ab, die einem Gartenzaun gleicht. Die Buchstaben des zu verschlüsselnden Textes werden abwechselnd in die (in der Regel) zwei Zeilen eingetragen und dann zeilenweise ausgelesen, also genau umgekehrt zur Spaltentransposition. Das Gartenzaunverfahren auf den Begriff „Kryptographie“ angewendet, sähe wie folgt aus.

K Y T G A H E

R P O R P I

Entsprechend lautet der Geheimtext: “KYTGAHERPORPI“. Auch für die Gartenzaun-Chiffre gibt es viele Variationsmöglichkeiten. Die einfachste Variation wäre eine Veränderung der Zeilenanzahl. Unterschiedliche Zeilenanzahlen liefern unterschiedliche Ergebnisse.

K P G P E

R T R H

Y O A I

[147] Wrixon, Fred: Geheimsprachen, S. 140 f.

Hier lautet der Geheimtext schließlich „KPGPERTRHYOAI“. Weitere Variationen sind beim Auslesen möglich. Man könnte beispielsweise die Zeilen rückwärts auslesen, oder im Wechsel eine Zeile vorwärts und die nächste rückwärts.

5.1.1.4. Fleissner-Verfahren[148]

Die Fleissner-Methode geht einen etwas anderen Weg. Zwar wird auch hier in eine Matrix geschrieben, die Matrix unterscheidet sich aber schon darin von den vorangegangenen Verfahren, dass sie quadratisch ist. Das Eintragen der Buchstaben geschieht mit Hilfe einer vorher erstellten Schablone. Diese Schablone (mit den gleichen Maßen wie die Matrix) wird auf die Matrix gelegt. Zeilenweise wird jeweils ein Buchstabe durch ein Loch geschrieben. Erreicht man das Ende der Schablone, so dreht man sie um 45° und schreibt wie der in der ersten Zeile beginnend weiter.

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Abbildung 4.3

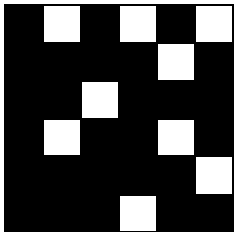


Abbildung 4.4

Die Abbildungen zeigen das grundsätzliche Raster und eine fertige Schablone. Legt man beide Zeichnungen übereinander, so stellt man fest, dass jede Zahl des linken Rasters genau einmal in der Schablone erscheint.

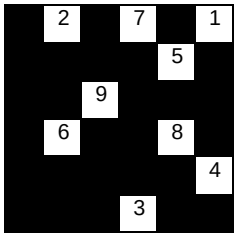


Abbildung 4.5

Dass dies so sein muss ergibt sich aus der Handhabung der Schablone. Denn jedes Mal, wenn man das Ende der Schablone erreicht (anders ausgedrückt: nach 9 eingetragenen Buchstaben) wird sie um 45° gedreht. Gleiche Zahlen im obigen Raster bedeuten, dass ein Loch durch die Drehung der Schablone auf diese Zahlen übergeführt wird. Z.B. wird ein Loch an Position 2 durch die Drehungen alle

[148] Fleissner von Wostrowitz, Eduard: Handbuch der Kryptographie, S. 65 ff.

Positionen erreicht, die mit 2 markiert sind. Daher darf eine Fleissner-Schablone keine zwei Löcher an Positionen besitzen, die mit derselben Nummer markiert sind. Würde man eine solche Schablone verwenden und einen Text eintragen, so gäbe es Felder, die nach einer Drehung bereits mit Buchstaben belegt sind. Dies kann in seltenen Fällen funktionieren, wenn nämlich rein zufällig die beiden Buchstaben an den beiden Positionen identisch sind, allerdings ist dies wirklich nur ein Zufall und liegt nicht im Sinne der Idee von Fleissner. Die optimale Schablone hat allerdings nicht nur keine zwei Löcher an Stellen, die durch Drehung ineinander übergeführt werden, sie hat auch immer die maximal mögliche Löcheranzahl. Bei obiger Schablone entspricht dies 9 Löchern (jede Zahl von 1 bis 9 liegt einmal frei). Hat die Schablone weniger Löcher, so ergeben sich im Geheimtext freie Felder. Die Anzahl der maximal möglichen Löcher ergibt sich aus der Größe der Schablone, bzw. der Anzahl der Felder insgesamt. Eine 8x8 Schablone hat insgesamt $8^2 = 64$ Felder. Diese Felderanzahl ergibt durch 4 geteilt (wegen der 4 Drehungen) 64:4 = 16 maximal mögliche Löcher. Man kann sich die 8x8-Schablone auch analog zur 6x6-Schablone oben in vier Bereiche eingeteilt vorstellen. Die Seitenlänge eines Bereiches ist dabei die Hälfte der gesamten Seitenlänge, in Feldern gesprochen also 4 Felder lang. Da auch diese Bereiche quadratisch sind ergeben sich schließlich wiederum $4^2 = 16$ Felder. Welche Felder nun letztlich ausgestanzt werden, spielt keine Rolle, solange die Regel beachtet wird keine zwei Felder mit gleicher Nummerierung auszustanzen. Es ist für Fleissner-Schablonen unüblich Quadrate mit ungerader Felderanzahl als Seitenlänge zu wählen, da der Mittelpunkt, um den die Schablone gedreht wird, dann mitten in einem Feld liegen würde, das seine Position niemals ändert. Man hätte also auch dann wieder das Problem, dass man ein Feld beschreibt, dass nach jeder Drehung offen aber bereits beschrieben ist. Die Drehung der Schablone erfolgt stets gegen den Uhrzeigersinn. Sind nach dem Eintragen aller Wörter noch Felder frei, so werden diese mit frei gewählten Buchstaben die keinen Sinn ergeben aufgefüllt. Schreibt man allerdings eine Nachricht die länger als die Anzahl der Felder ist, so hat man prinzipiell drei Möglichkeiten:

1. Man stellt sich eine neue, größere Schablone her.
2. Man verwendet die gleiche Schablone auf einer anderen Matrix und verschickt schließlich sämtliche beschriebenen Matrizen, oder

3. Man erstellt sich eine oder mehrere weitere Schablonen gleicher Größe und beschreibt damit die weiteren Matrizen (wobei man für jede Matrix eine neue Schablone verwendet).

Für den dritten Fall ergibt sich die Frage wie viele verschiedene solcher Schablonen eigentlich möglich sind. Dies hängt zunächst von der Größe der Schablone ab. Betrachten wir noch einmal die 6x6-Matrix vom Anfang. Jedes Feld darf nur einmal ausgestanzt werden, es muss aber auch genau einmal ausgestanzt werden. Dadurch ergeben sich 4 Möglichkeiten das Feld Nummer 1 auszustanzen. Gleiches gilt für Feld Nummer 2, Nummer 3 und alle anderen Felder auch. Wir haben also schließlich $4 * 4 * 4 * 4 * 4 * 4 * 4 * 4 * 4 = 4^9 = 262.144$ verschiedene Möglichkeiten eine solche Schablone herzustellen. Wählt man die Schablone entsprechend kleiner (4x4) oder größer (8x8) so ergeben sich auch weniger (4^4) oder mehr (4^{16}) unterschiedliche Möglichkeiten.

5.1.2. Monoalphabetische Substitutionschiffren

5.1.2.1. Atbash[149]

Atbash gehört zu den einfachsten oder naheliegendsten monoalphabetischen Substitutionsverfahren. Es findet sich an einigen Stellen in der Bibel (so z.B in Jeremia 25,26 und 51,41), weshalb es auch immer wieder als Bibelchiffre bezeichnet wird. Beim Atbash ist das Geheimtextalphabet die reversierte Darstellung des Klartextalphabets, mit anderen Worten dem ersten Buchstaben des Alphabets wird der Letzte zugeordnet, dem Zweiten der Vorletzte usw. Auf unser Alphabet angewendet sähe die Zuordnung wie folgt aus:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Abbildung 4.6

Für Alphabete mit ungeraden Buchstabenanzahlen ergibt sich bereits das erste Problem. Der Buchstabe der genau in der Mitte steht wird gar nicht erst, bzw. mit sich selbst, verschlüsselt. Eine Besonderheit stellt die Tatsache dar, dass dieses Verfahren involutorisch ist, das bedeutet, dass nicht nur der Schlüssel, wie bei symmetrischen Verfahren üblich, der gleiche ist, sondern auch die Vorgänge des Verschlüsselns und des Entschlüsselns identisch sind. Wendet man auf einen mit

[149] Singh, Simon: Geheime Botschaften, S 43.

Atbash verschlüsselten Text nochmals die Verschlüsselung an, so ist das Ergebnis also wiederum der Klartext.

5.1.2.2. Polybios-Tafel[150]

Polybios lebte von etwa 200 v. Chr. Bis 120 v. Chr. Er entwickelte ein Verfahren bei dem einzelne Buchstaben (Monogramme) durch Zahlenpaare (Bigramme) ersetzt wurden. Wegen der eindeutigen Zuordnung der einzelnen Buchstaben zu den Bigrammen gehört das Verfahren zu den monoalphabetischen Substitutionen. Polybios schrieb die Buchstaben in eine Tabelle deren Zeilen und Spalten er jeweils aufsteigend nummerierte. Ein Buchstabe wurde dann jeweils durch das durch die jeweilige Zeile und Spalte vorgegebene Zahlenpaar ersetzt.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abbildung 4.7

Das Wort „Tafel“ würde nach einer Durchführung des Verfahrens also mit den Zahlenpaaren „44 11 21 15 31“ dargestellt, oder ohne die Freizeichen „4411211531“.

5.1.2.3. Caesar-Verfahren[151]

Das Caesar-Verfahren ist wahrscheinlich das bekannteste monoalphabetische Substiutionsverfahren. Er wird oft auch als Verschiebechiffre bezeichnet. Beim Caesar-Verfahren wird ein Buchstabe des Klartextes durch einen Buchstaben des Geheimtextes verschlüsselt, wobei als Schlüssel die Differenz der beiden Stellen gilt. Ist der Schlüssel beispielsweise fünf, so wird jeder Buchstabe durch den Buchstaben ersetzt, der im Alphabet fünf Stellen hinter ihm steht. Caesar selbst wendete dieses Verfahren mit dem Schlüssel drei an. Zu jeder dieser Verschiebungen lässt sich eine Zuordnungstabelle erstellen.

[150] Wrixon, Fred: Geheimsprachen, S. 190 f.
[151] Selter, Christoph / Sundermann, Beate: HFIFJN! In: Die Grundschulzeitschrift 163/2003, S. 41 ff.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Abbildung 4.8

Es kann maximal 25 solcher Verschiebungen geben. Verschiebt man das Alphabet um 26 Stellen, so wird jeder Buchstabe wieder sich selbst zugeordnet. Interessant ist dieses Verfahren insbesondere in der Grundschule, denn hinter der Verschiebung steckt eine einfache Addition, die man durch eine andere Substitution deutlich machen kann.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Abbildung 4.9

In obiger Tabelle wird jedem Buchstaben die Zahl zugeordnet, an deren Stelle er im Alphabet steht. Die Verwendung der Addition in diesem Verfahren kann nun sichtbar gemacht werden, indem man den Klartext mit seiner Zahlenübersetzung aufschreibt, anschließend den Schlüssel hinzuaddiert und aus den entstandenen Zahlen schließlich den Geheimtext bildet. Die folgende Abbildung zeigt dieses Vorgehen.

Klartext	S	T	R	E	N	G	G	E	H	E	I	M
	19	20	18	5	14	7	7	5	8	5	9	13
+	5	5	5	5	5	5	5	5	5	5	5	5
Geheim-text	24	25	23	10	19	12	12	10	13	10	14	18
	X	Y	W	J	S	L	L	J	M	J	N	R

Abbildung 4.10

So genannte Caesar-Scheiben zeigen zu jeder Einstellung die passende Zuordnung. Man kann die Buchstaben dann einfach ablesen und muss nicht den Weg über die obige Addition gehen, außerdem kann man durch die Verschiebung schnell alle möglichen Zuordnungen sehen. Eine Variante der Caesar-Scheibe sieht vor, dass man als Geheimtextalphabet eine Permutation des Alphabets auf die Scheibe schreibt, sodass man den Geheimtext nicht durch die 25 Standartverschiebungen herausfinden kann. Gegen den Angriff mit einer Analyse der Buchstabenhäufigkeit bietet aber auch dieses Verfahren keinen größeren Schutz.

Das oben durchgeführte Additionsverfahren bietet hingegen die Möglichkeit mehrere Schlüssel in einer festen Reihenfolge zu verwenden, z.B. könnte man jeden zweiten

Buchstaben um zwei Stellen verschieben und die übrigen um vier Stellen. Für dieses Verfahren bietet sich die obige ausführliche Darstellung an, da man mit der Scheibe sonst für jeden einzelnen Buchstaben die Verschiebung neu durchführen müsste, was eventuell zu Verwirrungen führen kann.

5.1.2.4. Nomenklatoren[152]

Nomenklatoren stellen eigentlich eine Kombination mehrerer Verschlüsselungsverfahren dar. Häufig waren dies, insbesondere in der Anfangszeit, monoalphabetische Substitutionen. Was an den Nomenklatoren neu war, war, dass eine Art Katalog angelegt wurde um wichtige Begriffe komplett zu ersetzen. Dies konnten beispielsweise Personen oder Orte sein. Zu den bekanntesten Nomenklatoren gehört wohl die Geheimschrift Maria Stuarts, doch auch der Vatikan verwendete lange Zeit diese Methode. Aus ihnen sind später die umfangreichen Codebücher entstanden, die noch im Ersten und Zweiten Weltkrieg Verwendung fanden.

5.1.2.5. Buchchiffren

Buchchiffren sind Verfahren bei denen sich Absender und Empfänger zunächst auf ein gemeinsames Buch einigen. Oftmals werden dafür Wörterbücher verwendet, allerdings ist theoretisch jedes Buch für eine Buchchiffre geeignet. Der weitere Verlauf hängt davon ab, auf welche Vorgehensweise sich Absender und Empfänger einigen. Gemeinsam ist allen Buchchiffren, dass die Buchstaben im Klartext durch Zahlenwerte ersetzt werden, die mit Hilfe des Buches wieder dem Buchstaben zugeordnet werden können. Diese Angaben können beispielsweise „Seite, Zeile, Wort, Buchstabe“ sein. Es kann aber auch vorkommen, dass sich beide auf eine feste Seite einigen und die Worte ganz wegfallen lassen, sodass nur die Buchstaben in der Zeile abgezählt werden. Buchchiffren erfordern in der Regel einen großen Planungsaufwand, da all diese Kriterien zwischen Absender und Empfänger geklärt werden müssen, sonst ist dieser nicht in der Lage den Geheimtext zu entschlüsseln.

[152] http://de.wikipedia.org/wiki/Nomenklator, letzter Zugriff: 21.04.2009.

5.1.2.6 Freimaurerchiffre[153]

Die Freimaurerchiffre gehört zu den Symbolchiffren, da den Buchstaben des Klartextes hier keine Buchstaben oder Zahlen, sondern abstrakte Symbole zugeordnet werden. Die Zuordnung erfolgt aber wiederum monoalphabetisch. Bei der Freimaurerchiffre werden die Buchstaben in speziellen Tabellen angeordnet, die Position in der Tabelle ist eindeutig. Die Umrisse der Tabelle an dieser Stelle werden als Substitutionszeichen verwendet.

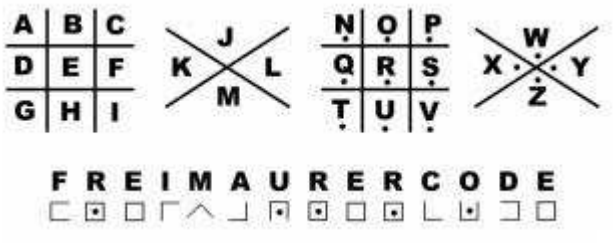


Abbildung 4.11

5.1.2.7. Playfair-Chiffre[154]

Die Playfair-Chiffre wurde eigentlich von Sir Charles Wheatstone erfunden. Sein guter Freund Lord Lyon Playfair erkannte jedoch das Potential und setzte sie beim britischen Militär durch. Aufgrund seines Einflusses in den oberen Kreisen und seines Einsatzes für die Chiffre, wird sie nach ihm und nicht nach dem Erfinder benannt. Die Playfair-Verschlüsselung erfolgt monoalphabetisch bigraphisch, d.h. es gibt zwar eine feste Zuordnung zwischen den Zeichen des Klartext- und Geheimtextalphabets, allerdings werden nicht mehr einzelne Zeichen verschlüsselt, sondern Zeichenpaare. Zu diesem Zweck wird zunächst der Klartext in Bigramme zerlegt. Satzzeichen werden dabei ausgelassen und der Buchstabe j durch i ersetzt. Sollte es zu Bigrammen aus zwei gleichen Buchstaben kommen, wird zu dessen Vermeidung ein x eingefügt. Genauso wird verfahren, wenn der Text nicht aufgeht und der letzte Buchstabe allein stehen bleibt. Es wird dann ein x am Ende eingefügt.
Aus „Substitution“ wird also „su bs ti tu ti on“.
Als nächstes wird das Playfair-Quadrat erstellt. Dieses Quadrat gleicht dem von Polybios, allerdings wird es mit einem frei wählbaren Schlüsselwort versehen. Die

[153] Wrixon, Fred: Geheimsprachen S. 183 f.
[154] Wrixon, Fred: Geheimsprachen, S. 217 ff.
Kippenhahn, Rudolf: Verschlüsselte Botschaften, S. 131 ff.

übrigen Buchstaben werden dann in ihrer Reihenfolge hinten angehängt. Ein Playfair-Quadrat mit dem Schlüsselwort „monoalphabetisch“ sähe wie folgt aus.

M	O	N	A	L
P	H	B	E	T
I	S	C	D	F
G	K	Q	R	U
V	W	X	Y	Z

Abbildung 4.12

Die Bigramme werden nach diesem Quadrat jeweils einzeln verschlüsselt. Für die Durchführung der Verschlüsselung wird zunächst überprüft, ob die beiden Buchstaben des Bigramms in einer Zeile oder Spalte stehen, oder ob sie das nicht tun. Stehen die beiden Buchstaben in einer Zeile, so werden sie durch ihre jeweils rechten Nachbarn ersetzt. Stößt man dabei an die Grenze des Quadrats, so fängt man wieder vorne an (aus SF wird beispielsweise CI). Stehen die beiden Buchstaben in einer Spalte, so ersetzt man sie durch ihre jeweils unter ihnen stehenden Nachbarn, erreicht man auch hier die Grenze verfährt man analog zu vorher. (aus QX wird XN). Stehen die beiden Buchstaben nicht in einer Zeile oder Spalte, so zeichnet man ein Rechteck über ihnen ein (oder man stellt es sich vor), wobei die beiden Buchstaben auf den diagonal gegenüber liegenden Ecken liegen. Die Buchstaben, durch die sie ersetzt werden, liegen dann auf den beiden anderen Ecken. Jedem Buchstaben wird der Buchstabe zugeordnet, der in seiner Zeile und in der Spalte des Anderen liegt (aus HQ wird also BK).

5.1.3. Polyalphabetische Substitutionschiffren

Bei polyalphabetischen Substitutionen findet die Buchstabenersetzung mit Hilfe mehrerer Geheimtextalphabete statt, der jeweilige Buchstabe wird also nicht mehr durch einen festen Buchstaben ersetzt, sondern durch mehrere, was einen Angriff über die Buchstabenhäufigkeit ausschließt.

5.1.3.1. Vigenère-Verfahren[155] und Vernam-Chiffre[156]

Vigenère entwickelte sein Verfahren nachdem er die Werke von Alberti, Porta und Trithemius studiert hatte. Er kombinierte die Tabula Recta von Trithemius mit dem Schlüsselwort von Porta und kommt somit zu seinem Verfahren. Dem Vigenère-Verfahren liegt also zunächst eine Tafel zugrunde.

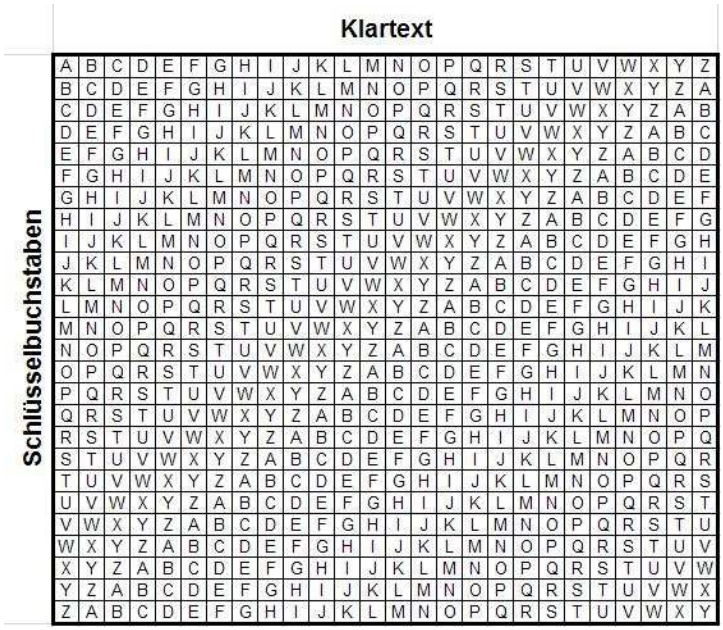


Abbildung 4.13

Nun wählt man ein Schlüsselwort. Dieses muss später auch dem Empfänger zugänglich gemacht werden. Nehmen wir an, der Klartext hieße „Vigenèretafel“ und das Schlüsselwort „Bauer“. Nun wird jedem Buchstaben des Klartextes ein Buchstabe des Schlüssels zugewiesen. Gelangt man ans Ende des Schlüssels, so beginnt man wieder von vorne.

V	I	G	E	N	E	R	E	T	A	F	E	L
B	A	U	E	R	B	A	U	E	R	B	A	U

Abbildung 4.14

Die Verschlüsselung erfolgt nun, indem man in der obersten Zeile des Feldes den Klartextbuchstaben sucht. Er markiert dann die entsprechende Spalte in welcher der verschlüsselte Buchstabe steht. Den Schlüsselbuchstaben sucht man in der vordersten Spalte. Er markiert die jeweilige Zeile. Der Buchstabe, der in der richtigen Spalte und Zeile steht, wird als Geheimtextbuchstabe verwendet. Im Beispiel markiert also das „V“ die Spalte und das „B“ die Zeile. Der Geheimtextbuchstabe

[155] Wobst, Reinhard: Abenteuer Kryptologie, S. 43 ff.
[156] Schmeh, Klaus: Kryptographie, 49.

lautet dann „W“. Fährt man mit dem Verfahren fort, so ergibt sich nach und nach der Geheimtext „WIAIEFRYXRGEF“. Hier wird die Stärke des Verfahrens deutlich. Im Geheimtext befinden sich nun einige Zeichen mehrfach (z.B. I, R, F, E). Diese Buchstaben stehen aber gerade nicht für jeweils den gleichen Buchstaben, sondern für unterschiedliche Buchstaben. Daher scheitert der Angriff über die Häufigkeitsanalyse. Gleichzeitig offenbart sich aber auch eine Schwäche des Verfahrens. Das Schlüsselwort „Bauer“ eignet sich nicht besonders für eine Vigenère-Verschlüsselung, da immer wenn ein „A“ im Schlüssel vorkommt, der ihm zugeordnete Buchstabe überhaupt nicht verschlüsselt wird, sondern im Geheimtext erhalten bleibt. In der Regel weiß dies zwar der Angreifer nicht, ist ihm dies aber bewusst, oder ahnt er das Vorkommen eines oder sogar mehrerer „A“ im Schlüssel, so sind dies Schwächen, die sich ausnutzen ließen.

Darüber hinaus bietet die Vigenère-Verschlüsselung heute auch keinen ausreichenden Schutz mehr, da mit Hilfe des Kasiski- und des Friedmann-Tests Rückschlüsse auf die Schlüssellänge gezogen werden können. Ist die Schlüssellänge bekannt, so beschränkt sich die Entschlüsselung des Vigenère-Verfahrens auf das Entziffern mehrerer monoalphabetischer Chiffren. Dies kann dann jedoch wieder über die Häufigkeitsanalyse geschehen. Wie der Kasiski-Test genau funktioniert, wird später erläutert, wichtig ist an dieser Stelle, dass sich wiederholende Folgen im Geheimtext ausgenutzt werden, um die Schlüssellänge zu berechnen.

Um solche verräterischen Wiederholungsfolgen gering zu halten oder gar zu vermeiden, ist es wichtig das Schlüsselwort möglichst lang zu wählen. Im Idealfall ist es sogar mindestens so lang wie der zu verschlüsselnde Text. Diese Variante nennt man dann Vernam-Chiffre nach dem Erfinder Gilbert Vernam. Doch auch die Vernam-Chiffre hält nicht jedem Angriff stand. Bestehen Klartext und Schlüssel aus normalen Sprachen, so sind die Buchstaben in ihnen wiederum ungleich verteilt. Ein Angreifer kann somit auch dieses Verfahren über eine Häufigkeitsanalyse brechen. Das ist zwar sehr kompliziert, aber im heutigen Computerzeitalter kein Kunststück mehr.

5.1.3.2. One-Time-Pad[157]

An dieser Stelle treten die One-Time-Pads auf den Plan. Sie wurden bereits 1917 von Major Joseph Mauborgne und Gilbert Vernam entwickelt. One-Time-Pads sind ebenfalls polyalphabetische Substitutionschiffren. Die Besonderheit ist, dass sie einerseits dem Prinzip der Vernam-Chiffre folgen, dass also das Schlüsselwort mindestens genauso lang ist wie die Nachricht, zum zweiten werden die Schlüssel aber absolut zufällig erzeugt, was einen Angriff über die Häufigkeitsanalyse ausschließt. Sie tragen den Namen One-Time-Pads, weil jeder zufällig generierte Schlüsselabschnitt nur ein einziges Mal verwendet werden darf und danach vernichtet werden muss. Würde man die jeweiligen Schlüssel oder Schlüsselabschnitte öfter verwenden, so hätten Kryptoanalytiker wieder Angriffspunkte über die Informationen, die ihnen der Geheimtext liefert. Verschlüsselt wird beim One-Time-Pad, indem man die Positionswerte des Klartext- und des Schlüsselbuchstabens addiert von der Summe und den Rest beim Teilen durch 26 ermittelt (also mod 26). Die neue Zahl entspricht der Positionsnummer des Geheimtextbuchstabens. Ich möchte das Verfahren an einem Beispiel verdeutlichen. Der Klartext soll „Caesar“ lauten, der Schlüssel „HDXJSK“ (wir gehen dabei davon aus, dass dieser Schlüssel wirklich zufällig ist. Für die beispielhafte Durchführung des Verfahrens an dieser Stelle spielt das ohnehin keine Rolle.)

C + H → 3 + 8 = 11 → 11 mod 26 = 11 → K

A + D → 1 + 4 = 5 → 5 mod 26 = 5 → E

E + X → 5 + 23 = 28 → 28 mod 26 = 2 → B

S + J → 19 + 10 = 29 → 29 mod 26 = 3 → C

A + S → 1 + 19 = 20 → 20 mod 26 = 20 → T

R + K → 18 + 11 = 30 → 30 mod 26 = 4 → D

Das verschlüsselte Wort lautet dann “KEBCTD”. Sieht man das Verfahren an einem Beispiel, wird auch deutlich, wieso es auf die Wichtigkeit des zufälligen Schlüssels ankommt. Mit Kenntnis der Sequenz ist es nicht schwer den Klartext wieder herzustellen. Ohne diese Kenntnis könnte der Schlüssel aber auch theoretisch „OZJOMQ“ geheißen haben. Dann wäre der Klartext aber nicht „Caesar“, sondern „Vernam“.

[157] Schneier, Bruce: Angewandte Kryptographie, S. 17 ff.

Das One-Time-Pad gilt damit als unknackbar, sofern man die nötige Sorgfalt an den Tag legt, da es aufgrund des völlig zufälligen Schlüssels nicht über eine Häufigkeitsanalyse gebrochen werden kann. Doch die Sicherheit, die der zufällige Schlüssel liefert, ist gleichzeitig das Problem des Verfahrens, denn man muss sich zunächst mal einen rein zufälligen Schlüssel generieren und das ist gar nicht so einfach. Das Naheliegendste ist oftmals die Verwendung des Computers zur Generierung einer zufälligen Buchstabenfolge und da liegt schon das erste Problem. Der Computer unterliegt gewissen Gesetzmäßigkeiten, die es ihm unmöglich machen echte Zufallszahlen zu produzieren. Dies bildet wiederum einen Angriffspunkt für die Kryptoanalytiker. Das Verfahren ist nur absolut sicher, wenn die Schlüsselfolge tatsächlich zufällig ist.

5.2. Moderne kryptographische Verfahren

In der Moderne regieren die Blockchiffren die Kryptographie. Claude Shannon forderte, dass der Geheimtext durch zwei bestimmte Vorgänge aus dem Klartext gebildet werden müsse: Konfusion und Diffusion[158]. Mit Konfusion meint Shannon eine Verschleierung des Zusammenhangs zwischen Klartextzeichen, Schlüsselzeichen und Geheimtextzeichen. Eine Substitution gilt beispielsweise als Konfusion. Diffusion bedeutet etwa die Verteilung der Klartextinformationen über den gesamten Geheimtext. Eine Form der Diffusion stellt die Transposition dar[159]. Blockchiffren nutzen die Technologie des Computers. Klartext, Schlüssel und Geheimtext werden nicht mehr in Form von Buchstaben oder Zahlen dargestellt, sondern in Bits[160]. Sie versuchen beide Grundsätze zu vereinen und chiffrieren darüber hinaus in vielen Runden um eine höhere Sicherheit zu gewährleisten.

5.2.1. Data Encryption Standart (DES)[161]

Beim DES werden 64-Bit-Blöcke verschlüsselt. Legt man also einen Klartext in Buchstabenform zugrunde (jeder Buchstabe ist im ASCII-Format durch 8 Bit verschlüsselt), so wird der Text in Blöcke zu je 8 Buchstaben aufgeteilt. Diese 64-Bit-

[158] Ertel, Wolfgang: Angewandte Kryptographie, S. 54.
[159] http://www.datenschutz-praxis.de/lexikon/k/konfusion.html, letzter Zugriff: 22.04.2009.
[160] Schmeh, Klaus: Kryptographie, S. 73.
[161] Schmeh, Klaus: Kryptographie, S. 74 ff.

Klartextblöcke werden über 64-Bit-Schlüsselblöcke (von denen allerdings 8 Bit Prüfbit darstellen, sodass der eigentliche Schlüssel nur 56 Bit Länge aufweist und damit kürzer als der Klartext ist) zu 64-Bit-Geheimtextblöcken verschlüsselt. Diese Blöcke werden zunächst einer Anfangspermutation unterzogen, die keinerlei kryptographische Bedeutung besitzt, da am Ende der Verschlüsselung eine zur Eingangspermutation inverse Endpermutation stattfindet.[162] Nach dieser Anfangspermutation wird der zu verarbeitende 64 Bit-Block nun in zwei Hälften zu je 32 Bit zerlegt. Anschließend durchlaufen die Blöcke eine Verschlüsselung die in 16 Runden wiederholt wird. Jede Runde beinhaltet folgende Vorgänge:

- Auf den rechten Block wird eine Funktion F angewendet. Das Ergebnis dieser Funktion wird mit dem linken Block exklusiv-oder (XOR) verknüpft und dieses Ergebnis schließlich zum neuen linken Block. (Exklusiv-oder beschreibt eine logische Verknüpfung. Auf den Bitbereich angewendet bewirkt die Schaltung den Ergebniswert ‚1', genau dann wenn die beiden Eingangswerte unterschiedlich sind, also ein Wert ‚1' und ein Wert ‚0' ist.)
- Der linke Block wird zum neuen rechten Block.

Die Funktion F bildet das eigentliche Kernstück des DES. Der rechte Block, der die Funktion durchläuft, wird zunächst permutiert und anschließend auf 48 Bit erweitert. Diese 48 Bit werden dann mit einem 48 Bit Stück des Schlüssels XOR verknüpft und danach in 8 Teilstücke zu je 6 Bit zerlegt. Jedes dieser 6 Bit Stücke leitet eine Substitution ein, deren Ergebnis ein 4 Bit Block liefert. Die nun vorliegenden 8 4 Bit-Blöcke ergeben zusammen wieder einen 32 Bit Block und den Ausgabewert der Funktion F.

Wenn ich gerade von einem 48 Bit Schlüsselteilstück gesprochen habe und zuvor von einem 56 Bit, bzw. 64 Bit Schlüssel, dann ist klar, dass auch der Schlüssel irgendeine Transformation durchmachen muss, bzw. dieses Teilstück irgendwie ausgewählt werden muss. Zunächst werden die 8 Prüfbits überprüft und (bei Korrektheit) verworfen. Aus dem verbleibenden 56 Bit Schlüssel müssen nun 16 solcher 48 Bit Teilschlüssel erstellt werden (für jeden Rundendurchlauf einen). Dazu wird der Schlüssel zunächst einer Permutation unterzogen und anschließend ebenfalls in zwei Teile aufgeteilt. Beide Teile leiten eine weitere Permutation ein, die zum ersten Teilschlüssel führt. In den Folgerunden werden die Hälften jeweils Bitweise rotierte und anschließend wiederum permutiert.

[162] Ertel, Wolfgang: Angewandte Kryptographie, S. 55.

Die folgende Abbildung zeigt noch einmal übersichtsartig den Ablauf des DES.

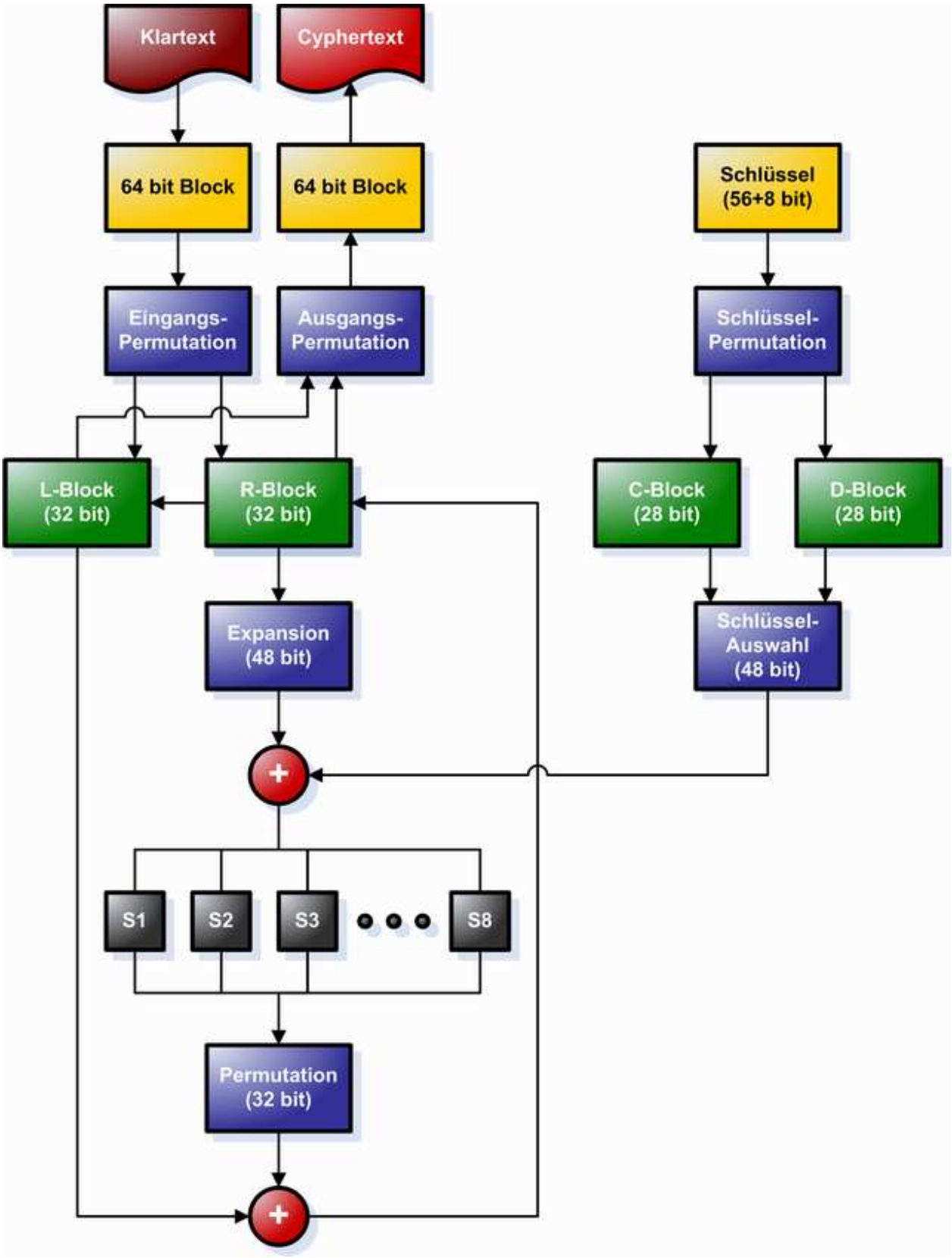


Abbildung 4.15

5.2.2. Advanced Encryption Standart (AES)[163]

Nachdem es Kryptoanalytikern gelungen war den DES schließlich doch zu knacken, wurde ein Wettbewerb um die Nachfolge dieses Verfahrens gestartet. Ein Verfahren mit Namen Rijndael von Vincent Rijmen und Joan Daemen gewann diesen Wettbewerb und wurde als Advanced Encryption Standart (AES) festgelegt. Rijndael unterstützt Blocklängen von 128, 192 und 256 Bit. In den AES wurde aber nur die 128 Bit Blocklänge aufgenommen. Allerdings lässt sich die Schlüssellänge zwischen 128, 192 und 256 Bit variieren. Genau wie beim DES werden auch beim AES mehrere Runden durchlaufen, wie viele das genau sind, hängt von der Länge des Schlüssels ab. Bei einem 128 Bit Schlüssel werden 10 Runden durchlaufen, bei einem 192 Bit Schlüssel sind es 12 und beim 256 Bit Schlüssel 14 Runden. Beim AES findet hingegen keine Aufteilung in rechten und linken Block statt, stattdessen wird der Block in einer 4x4-Matrix aufgebaut, die spaltenweise gefüllt wird. Aus dem Klartext (a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p) wird also die folgende Matrix:

a	e	I	m
b	f	j	n
c	g	k	o
d	h	l	p

Abbildung 4.16

Die Runden werden jeweils in vier Schritten durchlaufen. Zunächst wird eine Substitution durchgeführt, anschließend eine Transposition, der eine einfache Rotation der Zeichen einer Zeile um die Zeilenzahl nach links entspricht (wobei man sich die Zeilen mit 0 bis 3 nummeriert vorstellen muss), die erste Zeile wird also nicht rotiert, die zweite um ein Feld nach links verschoben, die dritte um zwei und die letzte um drei Felder. Im nächsten Schritt findet ein spaltenweises Durchmischen statt. Im letzten Schritt wird ein Teilschlüssel in Form einer exklusiv-oder Verknüpfung zur Matrix addiert. In der letzten Runde entfällt das spaltenweise Mischen, dafür wird der letzte Schritt doppelt durchgeführt, dadurch benötigt das Verfahren einen Teilschlüssel mehr als es Runden hat.

[163] Schmeh, Klaus: Kryptographie, S. 119 ff.

5.3. Schlüsselaustauschverfahren

Das Problem des Schlüsselaustauschs war lange Zeit das zentrale Problem der Kryptographie. Man hatte zwar mit der Verschlüsselung erreicht, dass der Angreifer die Nachricht nicht direkt abfangen und auslesen konnte, allerdings waren sämtliche Verfahren bis zur Neuzeit symmetrisch, sie nutzten also den gleichen Schlüssel zur Ver- und Entschlüsselung. Genauso wie die Nachricht selbst, so musste also auch der Schlüssel übertragen werden. Geschieht dies auf dem Kanal, der vom Angreifer abgehört wird, so ist die gesamte Verschlüsselung hinfällig, geschieht es auf einem nicht abgehörten Kanal, dann benötigt man die Verschlüsselung ohnehin nicht. Der Schlüssel muss also irgendwie sicher übertragen werden. Es galt lange Zeit als Paradoxon der Kryptographie, dass man zum sicheren Übermitteln einer Nachricht zwei verschlüsselte Nachrichten benötigte, nämlich die Nachricht selbst und den Schlüssel. Doch auch das Verschlüsseln des Schlüssels führt nicht zu einem befriedigenden Ergebnis, denn dabei entsteht ein neuer Schlüssel, der ebenfalls dem Empfänger mitgeteilt werden muss, damit er den ersten Schlüssel entschlüsseln kann. Bis weit ins 20 Jahrhundert hinein dachte man, dass es keine Lösung für den sicheren Schlüsselaustausch gäbe, bis zwei Kryptographen auf den Plan traten: Whitfield Diffie und Martin Hellman (eigentlich arbeiteten sie im Trio mit Ralph Merkle zusammen, allerdings hatte dieser wohl wenig Einfluss auf das Verfahren des Schlüsselaustauschs).

5.3.1. Diffie-Hellman-Schlüsselaustausch[164]

Diffie und Hellman kannten ein Verfahren, bei dem die sichere Übermittlung funktioniert ohne, dass der Schlüssel übertragen werden muss. Man stellt sich eine Kiste vor, in welche die Nachricht gelegt wird. Der Absender verschließt die Kiste mit einem Vorhängeschloss und schickt sie an den Empfänger. Dieser hängt sein eigenes Vorhängeschloss an die Kiste und schickt sie an den Absender zurück. Da die Kiste jetzt durch zwei Schlösser gesichert ist, kann der Absender sein Schloss wieder entfernen und der Inhalt bleibt weiterhin geschützt. Leider funktioniert dieses Verfahren in der Kryptographie nicht so einfach, denn im Gegensatz zum Beispiel ist in der Kryptographie das Vorgehen beim Entfernen der Schlösser nicht egal. Die

[164] Schmeh, Klaus: Kryptographie, S. 161 ff.

Entschlüsselung einer Nachricht muss dem LIFO (last in, first out) Prinzip folgen. Demnach muss die zuletzt angelegte Verschlüsselung zuerst entfernt werden, genau dann funktioniert obiges Verfahren aber nicht. Dennoch machte das Wissen um diese Funktionsweise Diffie und Hellman Mut und schließlich gelang es ihnen tatsächlich ein Verfahren zu entwickeln, dass ohne die Übergabe des Schlüssels auskommt.

Das Verfahren sieht wie folgt aus: Der Absender A und Empfänger E einigen sich auf eine Primzahl p und eine natürliche Zahl n mit n<p. Diese Einigung kann über einen ungesicherten Kanal erfolgen, da der Angreifer G, wie wir später sehen werden keinen Nutzen aus der Kenntnis ziehen kann. Nun wählt jeder der beiden am Vorgang beteiligten eine persönliche Zahl x<p, bzw. y<p, die er geheim hält. Nun berechnet der Absender $a = n^x \pmod p$ und der Empfänger $b = n^y \pmod p$. Die beiden Werte a und b werden wieder übertragen. An dieser Stelle liegt der Knackpunkt des Verfahrens. Die Berechnung von a und b findet über eine so genannte Einwegfunktion statt, das bedeutet, dass sie in einer Richtung relativ leicht durchzuführen ist, in der Gegenrichtung hingegen unmöglich, oder zumindest praktisch unmöglich. Simon Singh vergleicht die mathematische Einwegfunktion mit dem Mischen von Farben. Zwei Farben kann praktisch jeder zusammenmischen, es ist hingegen auf normalem Wege unmöglich die beiden Farben aus dem Ergebnis wieder herauszumischen.[165] Nun ist also A im Besitz von b und E im Besitz von a. Mit diesen Werten verfahren sie genau wie vorher, nur dass die Werte von a und b an die Stelle von n treten. A berechnet also $k_1 = b^x \pmod p$ und E berechnet $k_2 = b^y \pmod p$. Nach diesem Schritt gilt $k_1 = k_2$. A und E haben nun also den gleichen Wert berechnet, ohne ihn übertragen zu müssen. Diesen Wert können sie jetzt als sicheren gemeinsamen Schlüssel verwenden.

5.4. Die asymmetrische Verschlüsselung

Das Diffie-Hellman-Schlüsselaustauschverfahren ist zwar sicher, aber keineswegs bequem, da man nach wie vor Informationen zur Berechnung des gemeinsamen Schlüssels austauschen muss, was in unserer globalisierten Welt auch schon einmal dauern kann, man denke nur beispielsweise an die Zeitverschiebung. Wenn man mit jemandem einen gemeinsamen Schlüssel erzeugen möchte, der gerade schläft, weil

[165] Singh, Simon: Geheime Botschaften, S. 316.

es bei ihm drei Uhr nachts ist, dann erweist sich das ganze als etwas unpraktisch. Es war erneut Whitfield Diffie, der eine bahnbrechende Idee hatte. Er revolutionierte die Kryptographie, indem er von der symmetrischen Verschlüsselung wegkam. Diffie erwägte die Konzeption eines asymmetrischen Verfahrens, also einer Methode die zwei getrennte Schlüssel zum Ver- und Entschlüsseln verwendet. Unter diesen Umständen wäre es möglich einen Schlüssel zu veröffentlichen und den zweiten geheim zu halten. Die grundlegende Vorgehensweise bei der Verwendung einer solchen Verschlüsselung lässt sich relativ leicht an einer Analogie verdeutlichen. Man braucht sich nur einen Briefkasten vorzustellen. Das Einwerfen eines Briefes entspricht der Verschlüsselung mit dem allgemein zugänglichen Schlüssel. Das Leeren des Briefkastens kann hingegen nur der durchführen, der den privaten Schlüssel besitzt. Die Idee der Public Key Kryptographie war geboren. Nachdem das Verfahren und die Handhabung nun klar war, musste nur noch eine Möglichkeit gefunden werden, zwei Schlüssel zu erzeugen, die zueinander invers waren und bei denen man nicht vom später öffentlichen Schlüssel auf den privaten Schlüssel schließen konnte. Genau an diesem Punkt haperte es bei Diffie. Er stellte zwar ein solches Verfahren vor, dieses erwies sich jedoch nicht als angriffssicher.

5.4.1. Das RSA-Verfahren[166]

Was Diffie nicht gelang, schafften Ronald Rivest, Adi Shamir und Leonard Adleman am Massachusetts Institute of Technology. Das RSA-Verfahren ist eine Umsetzung der Public-Key-Idee von Diffie. Die Erstellung des Zahlenpaares geschieht wie folgt:

Man wählt zunächst zwei große Primzahlen p und q (groß bedeutet in diesem Zusammenhang mindestens über 100 Stellen, besser wären über 300 Stellen).
Nun berechnet man das Produkt der beiden Zahlen n = p*q, sowie das Produkt der beiden jeweils um 1 verkleinerten Faktoren f = (p-1) * (q-1).
Jetzt bestimmt man zwei Zahlen e und d für die gilt: e * d ≡ 1 (mod f).
Wählt man e als Primzahl kleiner f ergibt sich die Teilerfremde automatisch. Dann lassen sich Werte d und k finden, sodass sich mit Hilfe des erweiterten Euklidischen Algorithmus eine Vielfachsummendarstellung der Form e * d + f * k = 1 ergibt.

[166] Schneier, Bruce: Angewandte Kryptographie, S. 531 ff.
Ziegenbalg, Jochen: Public Key Cryptography, S.5 f.

Nach obiger Formel ist d invers zu e modul f. E, n und d sind dann unsere Schlüssel. E steht für encryption und bildet zusammen mit n den Schlüssel zum Verschlüsseln, d steht für decription und ist entsprechend der Schlüssel zum Entschlüsseln.
Die Verschlüsselung erfolgt schließlich wie folgt:
$c = m^e \bmod n$
Dabei ist m der Klartext und c der verschlüsselte Text. Die Entschlüsselung verläuft dann über die Invertierung:
$m = c^d \bmod n$.
Nach Verwerfung der nicht mehr benötigten Werte p und q ist das Verfahren insofern sicher, als dass sich aus der Kenntnis von e und n (die ja den öffentlichen Schlüssel bilden) d nicht berechnen lässt. Eine Berechnung ginge nur über die Zerlegung von n in p und q. Dies ist zwar rein theoretisch möglich, praktisch aber nicht umsetzbar, da es viel zu lange dauert. Ein Beispiel: Im Jahr 2005 gewann die Universität Bonn die RSA Factoring Challenge, indem sie eine 200-stellige Dezimalzahl faktorisierte. Sie begannen Ende des Jahres 2003. Die Faktorisierung war ihnen schließlich im Mai 2005 nach über einem Jahr Arbeit gelungen. Mittlerweile ist es den Wissenschaftlern der Universität Bonn gelungen eine Dezimalzahl mit über 1000 Stellen zu faktorisieren.[167] Das RSA-Verfahren ist damit theoretisch unsicher. Man macht sich aber die Tatsache zu nutze, dass die meisten verschlüsselten Nachrichten eine beschränkte Halbwertszeit haben. Unter Rücksichtnahme auf die weitere Entwicklung kann man die Primzahlen dann entsprechend so groß wählen, dass das Verfahren für die Dauer des Gebrauchs sicher ist.

6. Typische kryptoanalytische Verfahren

Im Bereich der Kryptologie gibt es zwei Seiten: Die Codemacher und die Codeknacker. Die Geschichte der Kryptologie zeigt, dass sich beide Parteien in einem wechselseitigen Spiel befanden, in dem jeder die Nase vorn haben wollte. Neue kryptographische Methoden forderten die Kreativität der Kryptoanalytiker. Anders herum waren die Kryptographen gezwungen sich neue Methoden auszudenken, wenn die alten Verfahren gebrochen worden waren.
Grundsätzlich lassen sich vier Angriffe auf Verschlüsselungen unterscheiden:

[167] http://de.wikipedia.org/wiki/RSA-Kryptosystem#Sicherheit_von_RSA, letzter Zugriff: 22.04.2009.

1. Ciphertext-Only-Attack: Bei diesem Angriff kennt der Kryptoanalytiker nur den verschlüsselten Text.
2. Known-Plaintext-Attack: Hier kennt der Angreifer neben dem verschlüsselten Text auch den Klartext. Aus dem Zusammenhang der beiden Texte lässt sich der Schlüssel erschließen.
3. Chosen-Plaintext-Attack: Der Angreifer hat die Möglichkeit aus einem gewählten Klartext einen verschlüsselten Text zu erstellen (beispielsweise bei Public-Key-Verschlüsselungen).
4. Chosen-Ciphertext-Attack: Hier hat der Angreifer die Möglichkeit aus einem verschlüsselten Text den Klartext zu erstellen.[168]
Ich möchte nun vier typische kryptoanalytische Verfahren erläutern, die zu der häufigsten Variante, dem Ciphertext-Only-Angriff, gehören.

6.1. Brute Force-Methode

Brute Force ist englisch und bedeutet soviel wie „rohe Gewalt“. Die Brute Force-Methode ist die Einfachste, gleichzeitig ist sie aber oftmals auch die Umständlichste oder zumindest Zeitaufwendigste. Brute Force ist nichts weiter als eine erschöpfende Suche, bei der alle möglichen Lösungswege durchlaufen werden, bis man den passenden Schlüssel gefunden hat. Für ein Zahlenschloss mit drei Ziffern bedeutet dies schlicht, simples probieren aller Kombinationen von 000 bis 999. Eine der Kombinationen muss ja die Richtige sein. An diesem kleinen Beispiel wird sofort der Zeitaufwand erkennbar. Brute Force liefert zwar bei endlichen Problemen stets eine Lösung, allerdings nur theoretisch. Ist der zu untersuchende Lösungsraum zu groß, so kann Brute Force schnell zu Laufzeiten führen, die nicht nur weit über ein Menschenleben hinausgehen, sondern auch über die geschätzte Existenzdauer des Universums.[169] Bei überschaubaren Problemgebieten ist sie hingegen die sicherste Methode, da sie stets zum Ziel führt. Die Skytale von Sparta ist ein Beispiel für ein kryptographisches Verfahren, dass für Brute Force anfällig ist. Man braucht nur die untereinander stehenden Buchstaben solange nebeneinander zu halten und zu verschieben, bis ein sinnvoller Text entsteht.

[168] Ertel, Wolfgang: Angewandte Kryptographie, S. 23
[169] Ziegenbalg, Jochen: Algorithmen. Von Hammurapi bis Gödel., S. 102 f.

6.2. Häufigkeitsanalyse

Die Häufigkeitsanalyse ist ein ganz klassisches kryptoanalytisches Werkzeug. Bereits im 7. Jahrhundert n. Chr. fanden arabische Gelehrte heraus, dass die Häufigkeit des Auftretens von Buchstaben für bestimmte Sprachen charakteristisch ist. Im Deutschen zum Beispiel ist „e“ der häufigste Buchstabe und „q“ der Seltenste. Dies schlägt sich natürlich in Texten nieder. Dieses Wissen lässt sich gegen monoalphabetische Substitutionen anwenden. Man muss nur wissen in welcher Sprache der Originaltext war. Wäre es beispielsweise ein deutscher Text, dann würde es keine Rolle spielen, ob in dem verschlüsselten Text der Buchstabe „p“ oder „z“ am häufigsten vorkommt, es wäre mit großer Sicherheit im Original das „e“ gewesen. Bei der Häufigkeitsanalyse zählt man also sämtliche Buchstaben und versucht eine eins-zu-eins-Zuordnung zu den Klartextbuchstaben nach der charakteristischen Verteilung zu schaffen. (Im Anhang zu dieser Arbeit befindet sich eine Tabelle mit der charakteristischen Buchstabenverteilung in der deutschen Sprache.)

6.3. Ermittlung der Schlüssellänge (Kasiski-Test)

Die Analyse der Buchstabenhäufigkeit funktioniert zwar bei monoalphabetischen Substitutionschiffren, sie versagt allerdings bei polyalphabetischen Substitutionen. Das ist auch nicht verwunderlich, denn die polyalphabetische Substitution war ein Ergebnis der Suche nach neuen Methoden, nachdem die monoalphabetischen Chiffren nicht mehr sicher waren. Doch auch polyalphabetische Chiffren, wie z.B. das Vigenère-Verfahren, bieten Angriffspunkte. Der Kasiski-Test ist ein Verfahren zur Bestimmung der Schlüsselwortlänge. Dabei sucht man im verschlüsselten Text nach sich wiederholenden Buchstabengruppen (mit mindestens drei gleichen Buchstaben). Je öfter man eine solche Buchstabengruppe findet, desto höher ist die Wahrscheinlichkeit, dass dies kein Zufall ist, sondern dass es sich um vielgenutzte Buchstabenkombinationen im Klartext handelt, die mit dem gleichen Teil des Schlüsselwortes verschlüsselt wurden. In der Folge zählt man den Abstand zwischen dem ersten Buchstaben der ersten Gruppe (inklusive) und dem ersten Buchstaben der nächsten Gruppe (exklusive). Diesen Vorgang führt man für jede Wiederholung durch. Dadurch erhält man eine Liste natürlicher Zahlen, die man nun in ihre

Primfaktoren zerlegt. Kommt ein Primfaktor häufig vor, dann weist dies darauf hin, dass es sich um die Länge des Schlüsselwortes handelt. Der Kasiski-Test liefert nämlich nicht automatisch die exakte Länge des Schlüsselwortes, er liefert auch Vielfache und Teiler der Länge. Allerdings lässt sich damit das Problem schon einschränken. Kryptologen empfehlen den Kasiski-Test mit dem Friedman-Test, der einen ungefähren Größenbereich für die Schlüsselwortlänge ergibt, zu kombinieren.[170] Hat man die Länge des Schlüsselwortes schließlich gefunden, so weiß man, das Buchstaben im Abstand der Länge des Schlüsselwortes mit dem gleichen Buchstaben verschlüsselt wurden. Man erhält also in der Folge eine Anzahl an monoalphabetischen Chiffrierungen, die man dann mit der Häufigkeitsanalyse relativ leicht knacken kann.

6.4. Cribs

Crib bedeutet eigentlich Krippe. Es kann aber auch Eselsbrücke heißen. Man könnte also sagen, dass man sich selbst eine Eselsbrücke erschafft. Am treffendsten für diese Methode ist allerdings der Ausdruck „crack a crib“ auf den Friedrich Bauer verweist. „To crack a crib“ bedeutet soviel wie „in ein Haus einbrechen“.[171] Cribs werden verwendet, um verschlüsselte Texte von Innen aufzuhebeln. Die Methode mittels Crib heißt Mustersuche, sie gehört zu einer speziellen Variante der Ciphertext-Only-Angriffe, zu den Probable-Plaintext-Attacks, also einem Angriff, der über mögliche Klartextstellen erfolgt. Bei der Häufigkeitsanalyse hatte ich erwähnt, dass eine bestimmte Buchstabenhäufigkeit charakteristisch für eine Sprache sei. Darüber hinaus gibt es aber auch Wörter die charakteristisch sein können, weil sie einfach oft vorkommen, z.B. die Artikel „der“, „die“ oder „das“. Der Hebel ist dabei die Vermutung, dass ein solches Wort einmal im Klartext vorkam. Man sucht dann nach Wiederholungen im Text mit der Anzahl der Buchstaben des Crib. Über die möglichen Positionen versucht man schließlich Rückschlüsse auf den Schlüssel zu ziehen. Geht man also davon aus, dass in einem Klartext zu einem verschlüsselten Text einmal das Wort Abrakadabra stand, dann sucht man im verschlüsselten Text nach Kombinationen der Form 12314151231. Lässt sich ein solches Wort im verschlüsselten Text lokalisieren, kann man dadurch einen Teil des Schlüssels entziffern. Von diesem Anfang aus, ist man oftmals in der Lage weitere Wörter durch

[170] Beutelspacher, Albrecht: Kryptologie, S. 32 ff.
[171] Bauer, Friedrich: Entzifferte Geheimnisse, S. 243.

logische Kombination zu erraten. Cribs waren für die Entschlüsselung der Enigma von besonderer Bedeutung. Dort waren es insbesondere Anredeformen und Wetterberichte gewesen, die die Cribs lieferten.[172]

7. Steganografie

Die Steganografie bildet den Teilbereich der Kryptologie, der sich nicht mit der Verschlüsselung von Nachrichten beschäftigt, sondern mit dem konkreten Verstecken von Nachrichten. Die Sicherheit steganografischer Methoden hängt davon ab, ob die Nachricht gefunden wird, also davon, wie gut das Versteck gewählt wurde. Ihre Stärke ist, dass ein eventueller Angreifer überhaupt nicht bemerkt, dass eine Nachricht transportiert wird, sodass er diesem Umstand gar keine Aufmerksamkeit widmet. Die große Schwäche: Wenn die Nachricht entdeckt wurde, dann liegt auch ihr Inhalt dem Angreifer offen, da dieser ja gerade nicht wie bei kryptographischen Verfahren verschlüsselt wurde.
Grundsätzlich lassen sich die steganografischen Methoden in drei Bereiche einteilen: die technische Steganografie, die linguistische Steganografie und die digitale Steganografie.[173]

7.1. Technische Steganografie

Die technische Steganografie umfasst die Methoden, bei denen eine geschriebene Nachricht im wörtlichen Sinne versteckt wird. Die Verfahren der technischen Steganografie sind vielfältig, denn sie besitzt hat von den drei Bereichen innerhalb dieser Wissenschaft die längste Tradition. Solche Verfahren wurden schon in der Antike verwendet, wenn auch nicht unter dem Begriff der Steganografie. Im Folgenden werden einige Methoden technischer Steganografie dargestellt.

7.1.1. Tätowierung von Sklaven

Zu den frühesten Belegen steganografischer Kunst gehört eine Überlieferung aus dem alten Griechenland, die zum Ionischen Aufstand führte. Histiaios, Herrscher von Milet, hatte den König der Perser, Darius I., auf seinen Feldzügen gegen die Skythen

[172] http://de.wikipedia.org/wiki/Mustersuche_(Kryptologie), letzter Zugriff: 16.04.2009.
[173] Schmeh, Klaus: Versteckte Botschaften, S. 217 f.

begleitet. Darius erkannte die Fähigkeiten von Histiaios und holte ihn als Berater an seinen Hof. Histaios hatte sich mehr erwartet und war über diese Entwicklung verbittert. Er wollte daraufhin seinen Schwiegersohn, der seine Führung in Milet übernommen hatte, zu einem Aufstand gegen die Perser bewegen, doch zwischen ihm und Milet lagen 1000 Kilometer. Ohne die Möglichkeiten globaler Vernetzung, die wir heute genießen, blieb Histiaios nur einen Boten zu schicken. Er wusste, wenn der Bote abgefangen und die Nachricht gefunden würde, dann würde das sein Ende bedeuten, also überlegte er sich eine Methode, wie er die Nachricht verbergen könnte. Er ließ einen treuen Sklaven zu sich bringen und ihm den Kopf rasieren. Auf den kahlen Kopf tätowierte er die Botschaft an seinen Schwiegersohn ein. Erst als die Haare nachgewachsen waren, entsandte er den Boten nach Milet. Niemand schöpfte Verdacht und als der Bote schließlich in Milet ankam, ließ er sich den Kopf erneut rasieren und die Nachricht kam zum Vorschein. Wenngleich Histiaios‘ Methode erfolgreich war, so lässt sich unschwer erkennen, dass sie sehr zeitintensiv war. Von der Niederschrift der Nachricht (also dem Vorgang des Tätowierens) bis zum Abschicken mussten Wochen, wenn nicht sogar Monate, ins Land gezogen sein, bis die Haarpracht so nachgewachsen war, dass niemand die Botschaft durch die Haare hindurch erkennen konnte. Für Histiaios war das egal, denn sein Plan musste nicht zeitnah umgesetzt werden, er wollte nur Rache für die Behandlung durch den Perserkönig und die bekam er auch. Für Botschaften, die dringlich sind und daher nicht so lange warten können, ist diese Methode allerdings ungeeignet.[174]

7.1.2. Wachstafeln

Eine solche Botschaft verschickte Demaratos. Demaratos war Grieche, doch er lebte im Exil in Susa, dort, wo der Königshof der Perser stand. Er fürchtete, dass der neue Perserkönig Xerxes I., der Darius I. nach dessen Tod in seinem Amt beerbt hatte, einen Krieg gegen Griechenland plane. Zwar wusste er nicht von konkreten Plänen, doch er bemerkte eine massive militärische Aufrüstung durch Xerxes und diese Truppen mussten ja auch einen Sinn haben. Demaratos entschloss sich eine Warnung in die alte Heimat zu schicken, doch auch er benötigte dafür eine sichere Methode. Demaratos hatte wohl keine Kenntnis über das Verfahren, dass Histiaios einige Jahre zuvor verwendet hatte, doch wenn er diese gehabt hätte ist dennoch

[174] Schmeh, Klaus: Versteckte Botschaften, S. 106.

fraglich, ob er sie auch eingesetzt hätte. Ein monatelanges Warten hätte vielleicht bedeutet, dass die Nachricht Griechenland zu spät erreicht. Demaratos kam auf eine andere Idee. Die Gelehrten der damaligen Zeit verwendeten zum Schreiben Wachstafeln, das waren Holztafeln, die mit Wachs überzogen waren. In das Wachs konnte der Text gekratzt werden und wenn man ihn nicht mehr brauchte, erhitzte man das Wachs einfach und ließ das flüssige Wachs wieder eine gleichmäßige Oberfläche bilden. Demaratos allerdings kratzte das Wachs komplett ab. Er ritzte seine Nachricht in das darunterliegende Holz und überzog es anschließend wieder mit der Wachsschicht, damit niemand Verdacht schöpfen würde. Die Tafel übergab er einem Boten und schickte diesen zu Leonidas von Sparta. Offensichtlich hatte Demaratos keinen treuen Sklaven, denn der Bote kannte das Geheimnis der Tafel nicht und auch Leonidas konnte nichts mit der leeren Wachstafel anfangen. Angeblich war es seine Frau, die auf die Idee kam das Wachs abkratzen zu lassen, sodass die verborgene Nachricht wieder zum Vorschein kam. Die Griechen hatten daraufhin Zeit sich auf den Angriff von König Xerxes I. vorzubereiten, der 480 v. Chr. stattfand.[175]

7.1.3. Die Skytale von Sparta

Eigentlich müsste ein Kapitel mit der Überschrift „die Skytale von Sparta“ im Bereich Steganografie verwundern, denn diese hatte ich bereits der Kryptographie zugeordnet und das auch mit gutem Grund, denn als eine der ersten Transpositionschiffren wurde die Skytale gerade dazu verwendet Nachrichten zu verschlüsseln und nicht zu verstecken. Doch die Spartaner erwiesen sich als weitsichtig, denn ihnen war durchaus bewusst, dass ein Skytaleband mit einer sinnlosen Anordnung von Buchstaben Aufmerksamkeit erregen würde, also kombinierten sie die kryptographische Methode der Skytale mit einem steganografischen Verfahren. Die Boten, die zur Überbringung der Botschaft eingesetzt wurden, verwendeten das Lederband, welches um die Skytale gewickelt und beschrieben worden war, oftmals als Gürtel. Indem sie die Seite mit den Buchstaben nach innen drehten, war das Band unauffällig getarnt. Damit waren die Nachrichten der Spartaner doppelt abgesichert. Eine solche, doppelt gesicherte, Botschaft soll den spartanischen Feldherrn Lysander vor einem Angriff von

[175] Schmeh, Klaus: Versteckte Botschaften, S. 107 f.

Pharnabasus gewarnt haben. Von den Spartanern ist darüber hinaus bekannt, dass sie Nachrichten in den Mägen frisch geschlachteter Tiere transportierten.[176]

7.1.4. Die Blase in der Ölflasche

Um etwa 350 v. Chr. veröffentlichte Aeneas der Taktiker sein Buch Poliorketika, welches eigentlich das korrekte Verhalten einer Bevölkerung bei der Belagerung ihrer Stadt beschreibt, allerdings gehört für Aeneas wohl auch das Übermitteln geheimer Nachrichten zu diesem richtigen Verhalten, denn er widmet einen großen Teil seines Buches eben kryptologischen Methoden, darunter eine Kryptographische und 15 Steganografische. Eines dieser steganografischen Verfahren funktioniert mit Hilfe der Blase eines toten Tieres und einer Ölflasche (damals noch undurchsichtig). Aeneas beschreibt, dass der Absender die Blase aufblasen und trocknen lassen soll. Anschließend solle er die Blase auf der Außenseite beschreiben und die Luft entweichen lassen. Die so zusammengefallene Blase kann dann in eine leere Ölflasche gegeben und soweit aufgeblasen werden, dass sie sich an die Wände der Flasche anlegt. Füllt man anschließend wieder Öl hinein, so wird die Flasche wieder ihrem ursprünglichen Zweck zugeführt, sodass niemand Verdacht schöpft in der Flasche könne eine Nachricht versteckt sein. Der Empfänger braucht dann nur das Öl aus der Flasche zu lassen und die Blase zu entfernen. Bläst er sie anschließend wieder auf, so kann er die Nachricht lesen.[177]

7.1.5. Das Ei des Giovanni Porta

Zu den wohl spektakulärsten steganografischen Methoden gehört eine aus dem 16. Jh. von dem großartigen Kryptologen Giovanni della Porta. Porta beschreibt im 16. Buch mit dem Titel „Of Invisible Writing“ seiner „Magia naturalis“ ein Verfahren mit dem man Nachrichten in ein Ei hinein schreiben kann. Dabei wird eine Mischung aus Essig und Alaun auf die Schale eines hartgekochten Eis aufgetragen. Die Flüssigkeit zieht dann durch die Schale hindurch und setzt sich auf der obersten Schicht des

[176] Singh, Simon: Geheime Botschaften, S. 23 f.
Schmeh, Klaus: Versteckte Botschaften, S. 109 f.
Wrixon, Fred: Geheimsprachen, S. 22.
[177] Schmeh, Klaus: Versteckte Botschaften, S. 110 ff.

harten Eiweißes ab. Schält man das Ei anschließend, so wird die Nachricht sichtbar.[178]

7.1.6. Geheimtinte

Zu den wohl bekanntesten Methoden technischer Steganografie gehört der Einsatz von Geheimtinte. Als Geheimtinte bezeichnet man Flüssigkeiten, die beim Schreiben keine sichtbaren Spuren hinterlassen. Es gibt eine ganze Liste von Flüssigkeiten die sich als Geheimtinte eignen, zu den bekanntesten zählen wohl Zitronensaft und Milch, doch auch einige pflanzliche Flüssigkeiten eignen sich zu dieser Verwendung. Um eine solche Geheimschrift sichtbar zu machen, benötigt man eine weitere Handlung. Oftmals handelt es sich dabei um Erhitzen der Nachricht, aber auch die Zugabe chemischer Stoffe führt manchmal zum gewünschten Erfolg. Die Geheimtinte hat eine lange Tradition. Die älteste, heute bekannte Erwähnung einer Geheimtinte findet sich bei dem Griechen Philon von Byzanz, der bereits im zweiten Jahrhundert vor Christus beschrieb, dass eine Flüssigkeit aus Galläpfeln sich zum unsichtbaren schreiben eignen würde. Diese Flüssigkeit lässt sich allerdings nicht durch Erhitzen sichtbar machen, sondern bedarf einer Substanz, deren Zusammensetzung er ebenfalls beschrieb.
Auch im römischen Reich waren Geheimtinten nicht unbekannt. Plinius der Ältere etwa berichtete von einer anderen Geheimschrift pflanzlicher Herkunft. Ovid hingegen empfahl den Einsatz von Milch. Doch dort bricht die lange Tradition der Geheimtinten nicht ab. Die berühmte Meisterspionin der Deutschen im Ersten Weltkrieg, Mata Hari, soll bei ihrer Festnahme eine Phiole Geheimtinte bei sich getragen haben. Heutzutage nimmt die Bedeutung der Geheimtinte ab, da die Verbreitung von Computer und Internet einerseits neue Methoden der Geheimhaltung ermöglicht und andererseits die Korrespondenz selbst häufig über die Datenautobahn erfolgt, wo Geheimtinten nicht eingesetzt werden können.[179]

7.1.7. Der Mikrofilm

Mit Mikrofilmen ist fast jeder schon einmal konfrontiert worden, der gerne Agentenfilme sieht. Die Datenspeicherung auf Mikrofilmen wird in der Filmindustrie

[178] Singh, Simon: Geheime Botschaften, S. 20
[179] Schmeh, Klaus: Versteckte Botschaften, S. 77 ff.

gerne für die Überbringung von Botschaften mittels Spionen verwendet. Dabei hat der Mikrofilm selbst zunächst überhaupt nichts mit geheimen Nachrichten zu tun, allerdings eignet er sich aufgrund seiner Größe deutlich eher dazu versteckt zu werden, als dies die größeren Pendants tun. Das hat nicht nur im Film zur Verwendung solcher Mikrofilme geführt, sondern auch in der Realität. Insbesondere zu Zeiten des Zweiten Weltkriegs und dem darauffolgenden Kalten Krieg wurde er gerne zur Spionage verwendet. Eines der bekanntesten Verstecke ist wohl der ausgehöhlte Schuhabsatz, doch auch viele andere Gegenstände bieten einem Mikrofilm genügend Platz zur unbemerkten Überbringung. Das Versteck im Schuh ist übrigens schon sehr viel älter. Bereits Aeneas der Taktiker schlug in seinem Buch Poliorketika vor, einem Sklaven Nachrichten in die ausgehöhlten Sandalen zu schieben.[180]

7.1.8. Der Mikropunkt

Emanuel Goldberg, ein in Moskau geborener Jude, stellte 1925 seine Erfindung auf einem Kongress in Paris vor. Goldberg hatte es geschafft Fotografien herzustellen, die auf der Größe eines Punktes eine ganze Seite ablichteten. Um das zu erreichen hatte er spezielle Linsen so angeordnet, dass sie ein verdrehtes Mikroskop darstellten. Alles wurde also stark verkleinert dargestellt. Durch dieses „Mikroskop“ hindurch fotografierte er die Seiten. Der Mikropunkt eignete sich hervorragend zur Übertragung geheimer Nachrichten. Er konnte beispielsweise als i-Punkt oder Satzpunkt in einem belanglosen Text platziert werden. Es wird auch berichtet, dass der Punkt in die gespaltenen Zacken einer Briefmarke eingebracht wurde. Eine so winzige Nachricht konnte praktisch überall versteckt werden, was die Nazis sich im Zweiten Weltkrieg zu Nutze. Dennoch entdeckten britische Aufklärer die Punkte irgendwann. Wie sie die ersten solcher Punkte in Briefen der Nazis entdeckten ist nicht bekannt, allerdings glänzten die Mikropunkte matt und es wird vermutet, dass eben dieser Glanz aufgefallen ist. Nachdem die ersten Mikropunkte entdeckt waren, wurden die Briefe der Nazis immer öfter auf Mikropunkte untersucht und es wurden auch viele davon entdeckt. Das Auslesen der Punkte stellte kein Problem dar, man musste den Punkt nur unter ein Mikroskop legen und vergrößern. Nach dieser Zeit stellte der Mikropunkt keine sichere Übertragungsmöglichkeit mehr dar, was auch die

[180] Schmeh, Klaus: Versteckte Botschaften, S. 29 ff.

Nazis feststellen mussten. Gegen Ende des Krieges nahm die Zahl der übermittelten Mikropunkte ab.[181]

7.2. Linguistische Steganografie

Ein weiterer steganografischer Bereich ist die linguistische Steganografie. Die linguistische Steganografie ist der Bereich, bei dem Nachrichten nicht im Klartext abgefasst und anschließend technische versteckt werden, sondern die Nachrichten selbst werden versteckt, z.B. durch markieren von Buchstaben in einem offenen Text, abbilden von Morsecodes in Bildern, usw. Die Linguistische Steganografie umfasst die beiden Teilgebiete „Semagramme“ und „Open Codes“.[182]

7.2.1. Semagramme

Von Semagrammen spricht man, wenn die Bedeutung einer in einem Text oder einer Abbildung versteckten Nachricht nicht von dem verwendeten Buchstaben oder Zeichen selbst abhängt, sondern von einer bestimmten Formgebung, seiner Position, oder einer Markierung. Semagramme lassen sich nahezu überall anbringen. Sie werden anhand ihres Trägermediums in Textsemagramme, Bildsemagramme und Gegenstandssemagramme unterschieden. Ein typischer Fall eines Textsemagrammes sind in einem Text markierte Buchstaben deren Aneinanderreihung die geheime Nachricht ergibt. Hier kommt es nicht konkret auf den Buchstaben an, sondern erst die Zusammensetzung der markierten Buchstaben liefert die Nachricht. Bildsemagramme gibt es in ganz unterschiedlichen Ausführungen. Ihre Codes können auch unterschiedliche Bedeutung haben. Die folgende Abbildung zeigt gleich drei Morsecodes. Das Bild stammt aus der französischen Zeitschrift Spirou.

[181] Schmeh, Klaus: Versteckte Botschaften, S. 87 ff.
[182] Schmeh, Klaus: Versteckte Botschaften, S. 217.

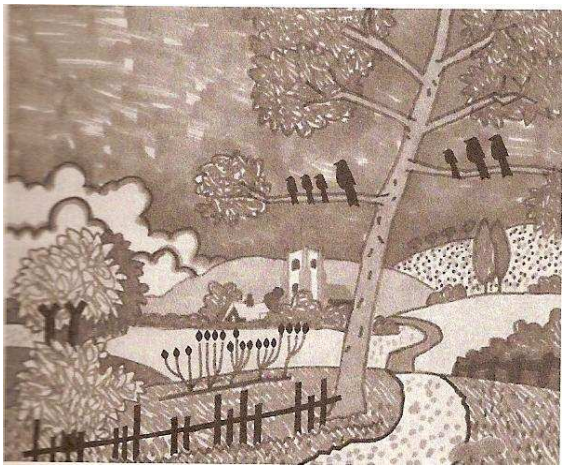


Abbildung 4.17

Ein Code versteckt sich in den schwarzen Raben, kleine Raben stehen dabei für Punkte und große für Striche. Ein weiterer Code findet sich in den Blumen unterhalb des Baumes, auch hier gilt: kleine Blumen bedeuten einen Punkt, Große einen Strich. Der letzte Code steckt schließlich in den Latten des Zaunes, er funktioniert nach der gleichen Regel. Die hier versteckten Morsecodes stehen für drei Automarken (Raben – VW, Blumen – Volvo, Lattenzaun – Buick). Ein Gegenstandssemagramm ließe sich zum Beispiel mit einer bestimmten Zeigerstellung bei Uhren verwirklichen. Das wussten auch die Amerikaner zur Zeit des Zweiten Weltkrieges, was dazu führte, dass bei Export-Uhren die Zeigerstellungen sicherheitshalber noch einmal verstellt wurden, bevor die Uhren zum Export freigegeben wurden.[183]

7.2.2. Open Codes

Open Codes sind Verfahren bei denen die geheime Botschaft in einem offenen Text versteckt ist. Open Codes lassen sich noch weiter unterteilen in Jargon-Codes, Null-Chiffren und Geometrische Codes.[184]

7.2.2.1. Jargon-Codes

Unter Jargon-Codes versteht man alle steganografischen Verfahren, bei denen einzelne Teile der offenen Nachricht (z.B. Sätze, Wörter, Zeichen oder Symbole) für den Eingeweihten eine andere Bedeutung haben. Ein relativ bekanntes Beispiel sind

[183] Schmeh, Klaus: Versteckte Botschaften, S. 18 ff.
[184] Schmeh, Klaus: Versteckte Botschaften, S. 217 f.

sogenannte Wettercodes. Sie sind deswegen so beliebt, weil sie sich zum einen hervorragend zum codieren eignen und zum anderen könnten die Wörter sogar teilweise gleich bleiben, was das Verfahren sehr einfach macht. „Heute stürmisches Wetter“ klingt zunächst so, als würde vor der Tür ein rauer Wind wehen. Der Satz könnte aber ebenso gut bedeuten, dass die Laune einer bestimmten Person heute mit Vorsicht zu genießen ist. Die Doppeldeutigkeit vereinfacht die Anwendung des Codes nicht nur, sie macht sie auch unsicherer, da aufgrund des verbreiteten Wissens um solche Doppeldeutigkeiten viele Leute auf die Idee kommen könnten den obigen Satz anders zu deuten. Wer auf Nummer sicher gehen will, der sucht sich abwegigere Kombinationen, das Verfahren bleibt allerdings das Gleiche.[185]

7.2.2.2. Null-Chiffren

Null-Chiffren sind sehr ähnlich wie Textsemagramme, es handelt sich also grundsätzlich auch um einen bestimmten Umgang mit Texten, allerdings kommt es hier nicht auf Formen oder Markierungen an. Von Null-Chiffren spricht man immer dann, wenn die Buchstaben der geheimen Botschaft im Text durch eine bestimmte, vorher festgelegte, Regel zu finden sind, also z.B. jeder erste Buchstabe eines Wortes, jeder letzte Buchstabe eines Wortes, jeder vierte Buchstabe eines Wortes, usw. Der folgende Text beinhaltet eine solche Nullchiffre:

„Gibt es heutzutage eigentlich interessante Mathematiker?“

Während die Fachwelt sich eine Diskussion über interessante Mathematiker der Gegenwart liefert, weiß der Eingeweihte bereits, dass es sich um eine geheime Botschaft handelt. Wer nämlich nur die Anfangsbuchstaben liest, erhält die Nachricht „geheim“.[186]

7.2.2.3. Geometrische Codes

Die Bezeichnung Geometrische Codes umfasst geheime Nachrichten, die mittels einer Schablone angefertigt und ausgelesen werden können. Worauf die Schablone gelegt wird (z.B. Bilder, Texte, etc.) spielt dabei keine Rolle. Die Geometrischen Codes der Steganografie scheinen damit der Fleissner-Schablone sehr ähnlich zu sein. Die Fleissner-Schablone ist aber eine kryptographische Verschlüsselung. Der

[185] Schmeh, Klaus: Versteckte Botschaften, S. 8 ff.
[186] Schmeh, Klaus: Versteckte Botschaften, S. 52 ff.

Unterschied zwischen der Fleissner-Methode und den geometrischen Codes liegt in der Geheimhaltung, man kann ihn am verschlüsselten Text erkennen. Ich hatte bereits ausgeführt, dass sich Kryptographie und Steganografie in der Art der Geheimhaltung unterscheiden. Während die Kryptographie darauf baut, dass ein Dritter zwar erkennt, dass er einen verschlüsselten Text vor sich hat, diesen aber nicht entziffern kann, liegt die Geheimhaltung bei steganografischen Verfahren darin dem Dritten die Kenntnis über eine geheime Botschaft vorzuenthalten. Dieser Unterschied wird in den beiden Schablonen-Verfahren deutlich. Führt man die Fleissner-Methode durch, so erhält man am Ende ein quadratisches Feld mit durcheinander geschriebenen Buchstaben (oder Zahlen, Zeichen, Symbolen, etc.). Die geometrischen Verfahren der Steganografie hingegen liefern wiederum einen sinnvollen Text, dessen Aussage jedoch für die geheime Botschaft nicht von Belang ist. Mit Hilfe der Schablone können dann die wichtigen Buchstaben erkannt und ausgelesen werden, sodass die Nachricht wieder zusammengesetzt werden kann. Klaus Schmeh subsumiert in seinem Buch „Versteckte Botschaften“ auch die Zinken unter die geometrischen Codes. Diese Einteilung erschließt sich mir nicht ganz. Zwar enthalten Zinken-Codes oftmals geometrische Zeichen oder Symbole, allerdings sind diesen Symbolen feste Aussagen zugeordnet. Man benötigt keine Schablone um sie auszulesen, sondern die Kenntnis um die Bedeutung der Zeichen selbst. Meiner Meinung nach gehören sie damit eher zu den Jargon-Codes.[187]

7.3. Digitale Steganografie

Statt digitaler Steganografie könnte man auch computergestützte Steganografie sagen, denn sie umfasst praktisch alle steganografischen Verfahren, die mit Hilfe eines Computers durchgeführt werden. Ein wichtiges Anwendungsgebiet der digitalen Steganografie stellen aber auch die digitalen Wasserzeichen dar.

7.3.1. Computerbasierte Steganografie

Als computerbasierte Steganografie bezeichnet man sämtliche steganografischen Verfahren, die dem eigentlichen Sinn der Steganografie folgen, also Nachrichten zu

[187] Schmeh, Klaus: Versteckte Botschaften, S. 40 ff.

verheimlichen (zur konkreten Differenzierung: also nicht die Zertifizierung) und die mit Hilfe eines Computers umgesetzt werden.

Der Computer liefert dafür heute ganz neue Möglichkeiten. Das Paradebeispiel hierfür dürfte das Verstecken von Nachrichten in digitalen Bildern sein. Bilder werden vom Computer in so genannten Pixeln dargestellt. Pixel sind einzelne kleine Bildpunkte die unterschiedlich farbig angesteuert werden können. Die Kombination vieler solcher einzelner farbiger Bildpunkte führt dann zu dem Bild selbst. Farben werden von einem Computer in einer bestimmten Codierung (meistens in einer Hexadezimalcodierung) abgespeichert bzw. aufgerufen. Durch den Hexadezimalcode weiß der Computer welche Einstellungen einzelner Bits er vornehmen muss um dem einen entsprechenden Bildpunkt die angeforderte Farbe zu geben. Die Farben werden dabei als Mischton aus den drei Grundfarben rot, grün und blau dargestellt. Jede einzelne Grundfarbe besteht aus acht Bit, also einem Byte, damit stehen jeder Farbe $2^8 = 256$ verschiedene Intensitäten zur Verfügung. Die Werte selbst liegen zwischen 0 und 255, wobei 0 bedeutet, dass die Farbe gar nicht zum Einsatz kommt und 255 einen sehr intensiven Farbton darstellt. Stehen alle drei Grundfarben auf 0, so ist das Ergebnis schwarz, stehen alle drei auf 255, so ist es weiß. Innerhalb einer Farbe sind die Bits einer speziellen Rangfolge zugeordnet. Ein höheres Bit verändert eine Farbe immer stärker als ein Niedrigeres. Da jedes Bit einen anderen Rang hat, gibt es also ein höchstes Bit, auch „most significant bit“ genannt und ein, niedrigstes, „least significant bit“. Eine Veränderung an dem most significant bit fällt dabei sofort auf. Je weiter das Bit hinten liegt, desto weniger fällt der Unterschied bei der Veränderung auf. Veränderungen an dem least significant bit sind für das menschliche Auge praktisch nicht mehr erkennbar. Diesen Umstand macht sich die computerbasierte Steganografie zu Nutze. Durch gezielte Veränderungen in den least significant bits wird das Bild zwar verändert, doch nur im technischen Bereich, nicht im optischen, gleichzeitig kann durch eine spezielle Codierung dieser Bits eine geheime Botschaft in ein Bild eingeschleust werden. Dies kann man mit speziellen Programmen erreichen. Wer von der versteckten Nachricht weiß, kann das gleiche oder ein ähnliches Programm benutzen um die Codierung der least significant bits und damit die Nachricht wieder auszulesen. Möglichkeiten der Manipulierung der least significant bits gibt es bei fast allen Dateiformaten, die mit solchen Codierungen arbeiten. Eine Computerdatei, die eine solche versteckte

Nachricht beinhaltet nennt man übrigens „cover“ (aus dem englischen „to cover“ = bedecken).
Eine andere computerbasierte Form der Steganografie, die an die Geheimtinte erinnert, ist die Möglichkeit in einem Textverarbeitungsprogramm Buchstaben in der Farbe des Hintergrundes einzufärben. Damit sind sie zwar nicht mehr zu sehen, wer aber weiß, dass solche Buchstaben oder Sätze in einem Text zu finden sind, der kann ihn an einem anderen Computer markieren und findet die versteckte Nachricht auf diese Weise sehr schnell.[188]

7.3.2. Digitale Wasserzeichen

Wasserzeichen kennt eigentlich jeder, der schon einmal einen Euroschein in der Hand hatte (viele andere Länder verwenden in ihrem Scheingeld ebenfalls Wasserzeichen, aber nicht alle). Wasserzeichen sind ein beliebtes Sicherheitskriterium, weil sie nicht direkt gesehen werden können, was einerseits dazu führt, dass der Anblick nicht verunstaltet wird und andererseits dazu, dass sie gegebenenfalls bei dem Versuch das Produkt zu kopieren übersehen werden und weil sie, wenn sie erkannt werden, dennoch nicht ganz einfach nachzumachen sind. Daher verwenden sie so viele Länder für ihr Scheingeld. Das Internet gehört ohne Frage zu den Bereichen unseres Lebens in denen täglich Millionen Kopien von Urheberrechtsverstößen begangen werden. Lange wusste man sich nicht dagegen zu helfen bis jemand auf die findige Idee kam, analog zu den Wasserzeichen auf dem Scheingeld, geheime Zeichen in digitale Dateien einzubauen, die eine Identifikation erleichtern und die Urheberschaft nachweisen können. Die digitalen Wasserzeichen fallen deswegen in den Bereich der Steganografie, weil sie eben auch in der Datei versteckt werden, sodass eine Person ohne Kenntnis diese Zeichen nicht bemerkt. Die Steganografie hat sich damit neue Einsatzgebiete erschlossen. Neben der Geheimhaltung von Nachrichten, dient sie nun auch der immer wichtiger werdenden Authentifizierung von Computerdateien im Internet. Die Methoden der digitalen Wasserzeichen sind dabei weitgehend identisch mit denen der computerbasierten Steganografie, allerdings müssen sie keiner Stegoanalyse standhalten, dafür müssen sie aber wenigstens so sicher sein, dass keiner das

[188] Schmeh, Klaus: Versteckte Botschaften, S. 150 ff.

Wasserzeichen entfernen kann, denn sonst ist die Urheberschaft ja wiederum nicht nachweisbar.[189]

7.3.3. Chaffing und Winnowing

„Chaffing and Winnowing“ sind eine besondere Form der Steganografie. Sie wurde von dem RSA-Miterfinder Ron Rivest entwickelt und so benannt. „To winnow the chaff from the wheat“ bedeutet in der englischen Sprache soviel wie „die Spreu vom Weizen trennen.“ Wenn „chaff“ also für die „Spreu“ steht und „winnow“ für die „Trennung“, dann bedeutet „Chaffing and winnowing“ soviel wie „mit Spreu versehen und wieder trennen“. Und genau das wird bei dieser Methode auch gemacht: Zu einem Klartext (z.B. Wir treffen uns um halb acht) wird eine sinnlose Nachricht erzeugt (z.B. Unser Lehrer gibt uns viele Hausaufgaben). Dabei kann die Nachricht selbst, wie im Beispiel, einen Sinn ergeben, nur nicht in Bezug auf den eigentlichen Klartext. Beide Nachrichten werden nun in Teile zerlegt, dabei ist wichtig, dass beide Texte in gleich viele Teile zerlegt werden. Das Beispiel ist so gewählt, dass beide Texte sechs Wörter haben, sodass wir sie in sechs Teile zerlegen:

Teil	Klartext	Zusatztext
1	Wir	Unser
2	treffen	Lehrer
3	uns	gibt
4	um	uns
5	halb	viele
6	acht	Hausaufgaben

Zu diesen Wörtern bilden wir nun jeweils eine Prüfsumme. In unserem Beispiel soll dies die Buchstabenanzahl des jeweiligen Wortes sein.

Teil	Klartext	Zusatztext
1	Wir (3)	Unser (5)
2	treffen (7)	Lehrer (6)
3	uns (3)	gibt (4)
4	um (2)	uns (3)
5	halb (4)	viele (5)

[189] Schmeh, Klaus: Versteckte Botschaften, S. 168 ff.

6 acht (4) Hausaufgaben (12)

Jetzt lassen sich die beiden Nachrichten zusammen bringen („chaffing“). Dabei bleibt die Reihenfolge der Teile gleich, allerdings könnte man die Texte nach der Prüfsumme ordnen. Der Text sieht dann folgendermaßen aus: Unser / wir , treffen / Lehrer , gibt / uns , uns / um , viele / halb , Hausaufgaben / acht. Nur wer jetzt die richtige Prüfsummenfolge kennt, nämlich 3, 7, 3, 2, 4, 4 kann die Nachricht auslesen („winnowing“). Obiges Beispiel zu knacken wäre nun prinzipiell kein Problem, allerdings wollte ich mit diesem Beispiel auch nur den Ablauf des Verfahrens erklären. Die Methode wird eigentlich so eingesetzt, dass der Klartext nicht in Wörter zerlegt wird, sondern in einzelne Bits zu denen dann sinnlose Bits generiert und eine Prüfsumme erstellt wird. Dann sieht die Sache schon etwas komplizierter aus. „Chaffing and winnowing“ stellt eine besondere Form der digitalen Steganografie dar, weil sie kein reines steganografisches Verfahren ist. Sinnlose Zeichen(-folgen) in einen Text einzubauen, um diesen unkenntlich zu machen ist eigentlich eine kryptographische Methode. „Chaffing and Winnowing“ schlägt also einen Spagat zwischen diesen beiden Gebieten.[190]

[190] Schmeh, Klaus: Versteckte Botschaften, S. 156 f.

V. Weitere Codierungsaspekte

Die Kryptographie ist eng mit dem Begriff der Codierung verknüpft, denn ein Code ist eine Übereinkunft über eine Reihe von Symbolen oder Lauten zur Übertragung von Informationen. Der Kommunikationsweg bedarf grundlegend drei Dingen: Erstens einen Absender, zweitens einen Empfänger und drittens einen entsprechenden Code auf den sich beide einigen, den also der Absender verwendet, um seine Information (im einfachsten Fall: in einem Gespräch) in Worte zu fassen und der Empfänger benutzt um die Worte zu dekodieren und damit zu verstehen. Das kommt dem Verschlüsselungsaspekt schon recht nahe. Der große Unterschied ist allerdings, dass die Verschlüsselung benutzt wird um Unbefugten die Kenntnis von der Information zu verheimlichen, während die Codierung ein wesentlicher Grundbestandteil sämtlicher Kommunikation überhaupt darstellt. So gesehen ist unsere Sprache ein Code, denn es ist nichts anderes als eine Vereinbarung im obigen Sinne. Gleiches gilt für unsere Schrift. Damit ergibt sich schließlich, dass die Kryptologie ein Teilgebiet der Codierung ist. Da auf ihr jedoch der Fokus liegt, habe ich sie diesem Kapitel vorangestellt. Dennoch darf auch der Codierungsaspekt nicht vergessen werden. Gründe für Codierung sind zum Beispiel durch technische Neuerungen geboten (z.B. beim Morse-Code) oder werden zum Zwecke der Kompression der heute unglaublichen Datenmengen verwendet (z.B. Huffmann-Code). Es kann aber auch vorkommen, dass bestimmte Wege der Kommunikation gestört sind, sodass man auf andere Wege ausweichen muss (man bedenke nur den Einsatz von visuellen Flaggenalphabeten auf Flugzeugträgern, da der Pilot den Einweiser nicht hören kann, oder auch die Brailleschrift für Blinde).

Wer mit offenen Augen durch die Welt läuft, der kommt nicht umhin an jeder Ecke Codes zu sehen: Straßennamen, Hausnummern, Telefonnummern, Rückennummern von Fußballspielern, die Artikelnummern von Waren im Supermarkt und vieles mehr. Einige Codes, die für uns von besonderer Bedeutung sind, möchte ich im Folgenden vorstellen.

1. Brailleschrift

Die Brailleschrift ist nach ihrem Erfinder benannt. Louis Braille entwickelte diese Schrift 1825 für sehbehinderte Menschen. Sie besteht aus einem Muster von 6 Punkten, die ähnlich der 6 auf unseren Würfeln angeordnet sind. Mit diesen Punkten lassen sich 2^6 = 64 Zeichen darstellen. Diese Zeichen beinhalten grundlegend die Buchstaben, sowie Ziffern und einige Sonderzeichen. Die Darstellung der codierten Zeichen erfolgt, indem man die zu dem Zeichen gehörenden Punkte von hinten in die Unterlage presst, sodass man sie von vorn ertasten kann. Die folgende Abbildung zeigte die deutsche Version der Brailleschrift.

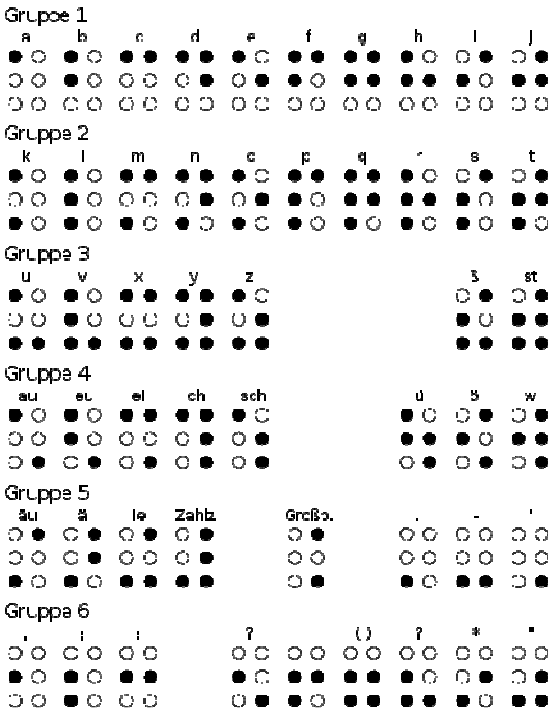


Abbildung 5.1

Die Brailleschrift ist ein gutes Beispiel für die enge Verwandtschaft zwischen Codierung und Kryptographie, denn wer den Braille-Code nicht kennt, für den sind die Punktmuster kaum zu entziffern. Dennoch fehlt dem Braille-Code das Geheimhaltungsmotiv. Die Schrift wurde ja gerade nicht zu kryptographischen Zwecken entwickelt, sondern um sehgeschädigten Menschen die Möglichkeit zu geben, Schrift wahrzunehmen. Die Information soll also gerade verbreitet werden. Heutzutage gibt es für viele Länder eigene Brailleschrift-Codes, da sie unterschiedliche Buchstaben besitzen (z.B. die Umlaute in der deutschen Sprache), außerdem wurde die Brailleschrift für die Arbeit am Computer, bei der mehr

Sonderzeichen benötigt werden um eine Zeile (also zwei weitere Punkte) erweitert. Mit dieser Variante lassen sich entsprechen 2^8, also 256 Zeichen darstellen.[191]

2. Morse-Code

Der amerikanische Erfinder Samuel Morse hatte 1833 den Telegrafen erfunden. Vier Jahre später wurde der erste Test mit einer frühen Version des Morse-Code durchgeführt. Grundlage für den Morse-Code ist zunächst ein binäres System, also eines, welches zwei verschiedene Zustände annehmen kann (bei einem Licht beispielsweise „Licht an“ und „Licht aus“). Hinzu kommt, dass der Morse-Code zwei Zustände in der Länge des eingeschalteten Signals unterscheidet, nämlich „lang“ und „kurz“. Insgesamt werden bei der Verwendung des Morse-Codes also drei unterschiedliche Zustände unterschieden: „Signal aus“, „kurzes Signal“ und „langes Signal“. Da der Morse-Code keine maximale Signalbeschränkung hat, kann man nicht so einfach ermitteln, wie viele Zeichen man mit ihm darstellen kann, wie dies z.B. bei der Brailleschrift der Fall war. Theoretisch sind es unendlich viele. Die folgende Abbildung zeigt die Standartcode-Tabelle.

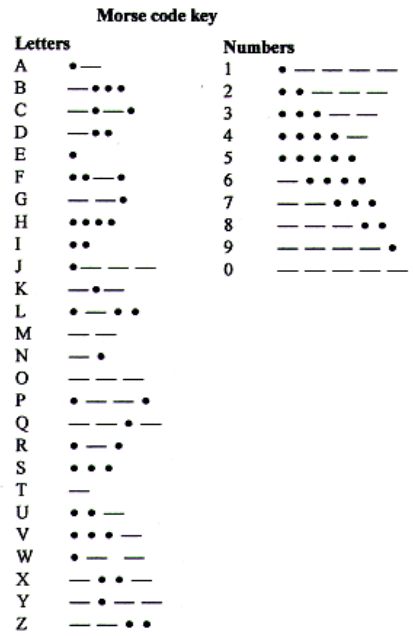


Abbildung 5.2

Zwar wurde der Morse-Code zu Kriegszeiten auch als kryptographisches Mittel eingesetzt, doch sein Codierungsaspekt überwiegt dermaßen stark, dass ich ihn hier

[191] http://de.wikipedia.org/wiki/Brailleschrift, letzter Zugriff: 14.04.2009.

eingeordnet habe. Dieser Code diente nämlich insbesondere zur Übertragung über weite Strecken hinweg mittels Impulse durch die Telegrafenleitungen. Wie wertvoll diese schnelle Technik zur Informationsübermittlung war, lässt sich am Sezessionskrieg erkennen.[192]

3. Genetischer Code

Ein Biologe würde mit dem Begriff „Code“ vielleicht zunächst den „genetischen Code“ assoziieren. Dabei werden die in unseren Genen enthaltenen Aminosäuren durch drei aufeinanderfolgende Nukleinbasenpaare codiert. Diese sind Adenin, Guanin, Cytosin, sowie Uracil in der RNS (Ribonukleinsäure), bzw. Thymin in der DNS (Desoxyribonukleinsäure). Die Anfangsbuchstaben der jeweiligen Begriffe werden dabei als Kürzel verwendet, sodass man Buchstabentripel wie GAU (hier nicht „Größter anzunehmender Unfall“, sondern die Codierung der Asparaginsäure) erhält. Die folgende Abbildung zeigt die sogenannte „Genetische Code-Sonne“. Die Nukleobasen werden von innen nach außen abgelesen.

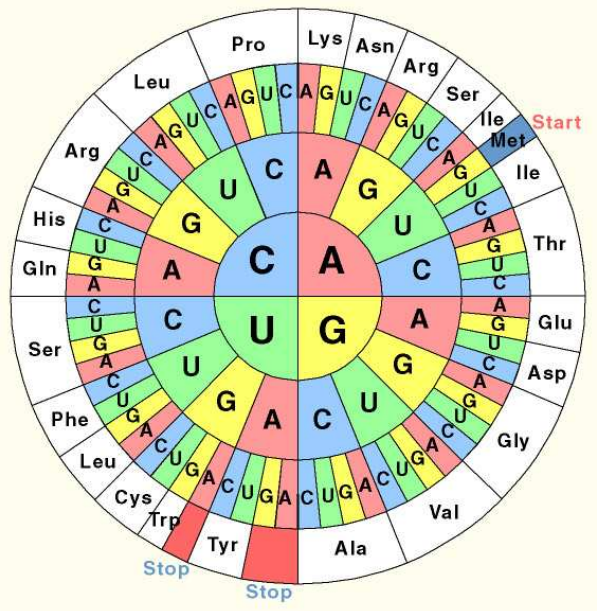


Abbildung 5.3

Der genetische Code ist sicherlich kein Beispiel für eine Codierung, die uns im Alltag begegnet, er ist allerdings nicht nur von besonderer Bedeutung für die Wissenschaft, sondern zeigt auch in wie vielen Bereichen Codes zum Einsatz kommen.[193]

[192] http://de.wikipedia.org/wiki/Morsecode, letzter Zugriff: 14.04.2009.
[193] http://de.wikipedia.org/wiki/Genetischer_Code, letzter Zugriff: 14.04.2009.

4. Duales Zahlensystem

Das duale Zahlensystem wurde erstmals von Gottfried Wilhelm Leibniz Ende des 17., Anfang des 18. Jahrhunderts vollständig ausgearbeitet. Es ist deswegen heute so bedeutsam, weil es die Grundlage der heutigen Computer bildet. Konrad Zuse gilt heute als der Erfinder des ersten frei programmierbaren Computers. Seine Maschine Z3 wurde 1941 fertig gestellt. Bereits damals forderte Zuse, dass Rechenmaschinen mit dem dualen Zahlensystem arbeiten sollten. Duales System bedeutet, dass es nur zwei Elemente besitzt. Beim dualen Zahlensystem sind dies die Werte 0 und 1. Diese Werte lassen sich bestimmten Zuständen zuordnen, z.B. 0 es fließt kein Strom und 1 es fließt ein Strom. Diese Zustände können in der Maschine Computer weitergeleitet und verarbeitet werden.

Die Darstellung erfolgt analog zu unserem Zehnersystem stellengerecht. Die Zahl 345 entspricht im Dezimalsystem $3 * 100 + 4 * 10 + 5 * 1$ oder anders dargestellt: $3 * 10^2 + 4 * 10^1 + 5 * 10^0$. Im Binärsystem fehlen die Ziffern 3, 4 und 5. Die Ziffernfolge 11010 allerdings bedeutet $1 * 2^4 + 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0$, was der Zahl 25 in unserem System entspricht. Das Zweiersystem ist also eine 2-adische Zahldarstellung. Man spricht auch vom Stellenwertsystem zur Basis 2.

Es existieren unterschiedliche Codes für die Zahldarstellung im Zweiersystem. Der wohl bekannteste dürfte der BCD-Code sein. BCD steht für „binary coded decimals“. Es ist die natürliche Darstellung unserer Zahlen im Zweiersystem.

Ein anderer binärer Zahlencode ist etwa der, von dem amerikanischen Computerpionier Howard Aiken entwickelte, Aiken-Code. Beim Aiken-Code werden die von 0 aufsteigenden Ziffern gespiegelt (also Einsen und Nullen vertauscht) und für die von 9 absteigenden Ziffern verwendet. Die ersten fünf Zahlen sehen damit genauso wie beim BCD-Code aus. Die hinteren Fünf ergeben sich dann aus der Symmetrie. Der Aiken-Code kommt noch heute in Digitaluhren und Taschenrechnern zur Anwendung.[194]

Der Physiker Frank Gray entwickelte ebenfalls einen nach ihm benannten Code. Die Besonderheit beim Gray Code liegt darin, dass sich eine Zahl von ihrem Vorgänger nur an einer Stelle, also in einem Bit unterscheidet. Dieser Code soll Fehler verringern und kommt insbesondere bei der Übertragung digitaler Signale über

[194] http://de.wikipedia.org/wiki/Aiken-Code, letzter Zugriff: 15.04.2009.

analoge Wege, also bei einer Translation digitaler Signale in Analoge, zum Einsatz.[195]

Der Exzess-3 Code, oder nach dem Entwickler George Stibitz benannte Stibitz-Code, will vor allem einige unerwünschte Begleiterscheinungen vermeiden. In technischen Anwendungen stehen die Halbbytes 0000 und 1111 oftmals für die Unterbrechung des Stromflusses sowie einen Dauerton. Der Wert 1111 wird zwar nur beim Aiken-Code erreicht, 0000 allerdings bei allen drei zuvor genannten Codes. Um diese Werte zu umgehen, wird jeder Tetrade der Wert drei hinzuaddiert. Die binäre Darstellung der drei lautet 0011. Die Werte sehen dann wie folgt aus.

Dezimalzahl	BCD-Code	Exzess-3 Code	Aiken Code	Gray Code
0	0000	0011	0000	0000
1	0001	0100	0001	0001
2	0010	0101	0010	0011
3	0011	0110	0011	0010
4	0100	0111	0100	0110
5	0101	1000	1011	0111
6	0110	1001	1100	0101
7	0111	1010	1101	0100
8	1000	1011	1110	1100
9	1001	1100	1111	1101

Abbildung 5.4

5. Hexadezimalsystem

Das Arbeiten im Dualsystem ist zwar für die Maschine von grundlegender Bedeutung. Für uns Menschen ist diese Darstellung allerdings oftmals unständlich. Für die Arbeit am PC hat sich daher der Einsatz des Hexadezimalsystems, also eines Systems zur Basis 16, bewährt. Dies bietet sich an, weil 16 ein Vielfaches von 2 ist, denn $2^4 = 16$. Entsprechend kann ein Byte, also nicht nur in Form von 8 aufeinander folgenden Nullen und Einsen dargestellt werden, sondern auch durch zwei hexadezimale Werte. Die Darstellung in zwei Zeichen ist komfortabler, als die in Acht. Da in unserem Dezimalsystem aber Ziffern für die Werte größer 9 fehlen, werden die weiteren Zahlen bis 15 durch die Buchstaben A bis F ersetzt.

Dezimalzahl	Hexadezimalzahl
0	00

[195] Ziegenbalg, Jochen: Codierung und Kryptographie, S. 9.

1	01
2	02
3	03
4	04
5	05
6	06
7	07
8	08
9	09
10	0A
11	0B
12	0C
13	0D
14	0E
15	0F

Abbildung 5.5

6. ASCII und UNICODE

Am Aufstieg des Computers wollten viele teilhaben, also stiegen sie in den Markt ein und produzierten eigene Geräte. Die Geräte brauchten Zeichensätze zum Erkennen der Eingabe. Praktisch jeder Hersteller hatte seinen eigenen Zeichensatz, was dazu führte, dass die Computer untereinander weitgehend inkompatibel waren, sofern sie nicht vom gleichen Hersteller stammten. Eine Normierung des Zeichensatzes wurde unausweichlich. Diese Norm bildete der 1967 veröffentlichte ASCII. ASCII steht für „American Standart Code for Information Interchange“. Der ASCII ist ein 7-bit Code. Mit ihm lassen sich also 2^7 = 128 Zeichen darstellen, davon sind 33 Zeichen Steuerbefehle (wie z.B. der Zeilenumbruch). Die übrigen Zeichen umfassen das im englischen gebräuchliche lateinische Standardalphabet (also ohne unsere Umlaute) in großen, wie in kleinen Buchstaben, die zehn arabischen Ziffern und einige Sonderzeichen, wie Klammern, Plus, Minus, Gleichheitszeichen, Punkt, Komma, usw.

000	NUL	033	!	066	B	099	c	132	ä	165	Ñ	198	ã	231	þ
001	Start Of Header	034	"	067	C	100	d	133	à	166	ª	199	Ã	232	Þ
002	Start Of Text	035	#	068	D	101	e	134	å	167	º	200	╚	233	Ú
003	End Of Text	036	$	069	E	102	f	135	ç	168	¿	201	╔	234	Û
004	End Of Transmission	037	%	070	F	103	g	136	ê	169	®	202	╩	235	Ù
005	Enquiry	038	&	071	G	104	h	137	ë	170	¬	203	╦	236	ý
006	Acknowledge	039		072	H	105	i	138	è	171	½	204	╠	237	Ý
007	Bell	040	(	073	I	106	j	139	ï	172	¼	205	═	238	¯
008	Backspace	041	)	074	J	107	k	140	î	173	¡	206	╬	239	´
009	Horizontal Tab	042	*	075	K	108	l	141	ì	174	«	207	¤	240	
010	Line Feed	043	+	076	L	109	m	142	Ä	175	»	208	ð	241	±
011	Vertical Tab	044	,	077	M	110	n	143	Å	176	░	209	Ð	242	‗
012	Form Feed	045	-	078	N	111	o	144	É	177	▒	210	Ê	243	¾
013	Carriage Return	046	.	079	O	112	p	145	æ	178	▓	211	Ë	244	¶
014	Shift Out	047	/	080	P	113	q	146	Æ	179	│	212	È	245	§
015	Shift In	048	0	081	Q	114	r	147	ô	180	┤	213	ı	246	÷
016	Delete	049	1	082	R	115	s	148	ö	181	Á	214	Í	247	¸
017	-- frei --	050	2	083	S	116	t	149	ò	182	Â	215	Î	248	°
018	-- frei --	051	3	084	T	117	u	150	û	183	À	216	Ï	249	¨
019	-- frei --	052	4	085	U	118	v	151	ù	184	©	217	┘	250	·
020	-- frei --	053	5	086	V	119	w	152	ÿ	185	╣	218	┌	251	¹
021	Negative Acknowledge	054	6	087	W	120	x	153	Ö	186	║	219	█	252	³
022	Synchronous Idle	055	7	088	X	121	y	154	Ü	187	╗	220	▄	253	²
023	End Of Transmission Block	056	8	089	Y	122	z	155	ø	188	╝	221	¦	254	■
024	Cancel	057	9	090	Z	123	{	156	£	189	¢	222	Ì	255	
025	End Of Medium	058	:	091	[	124	|	157	Ø	190	¥	223	▀		
026	Substitude	059	;	092	\	125	}	158	×	191	┐	224	Ó		
027	Escape	060	<	093	]	126	~	159	ƒ	192	└	225	ß		
028	File Seperator	061	=	094	^	127	⌂	160	á	193	┴	226	Ô		
029	Group Seperator	062	>	095	_	128	Ç	161	í	194	┬	227	Ò		
030	Record Seperator	063	?	096	`	129	ü	162	ó	195	├	228	õ		
031	Unit Seperator	064	@	097	a	130	é	163	ú	196	─	229	Õ		
032		065	A	098	b	131	â	164	ñ	197	┼	230	µ		

Abbildung 5.6

Der ASCII war ein großer Fortschritt für die Computerindustrie und insbesondere auch für die Benutzer der Computer, da durch die Standardisierung nun Projekte auf unterschiedlichen Rechnern liefen und auch erarbeitet werden konnten.

Doch der Boom der Computerindustrie ging weiter und wieder einmal stand man vor einem Problem: Der ASCII hatte zwar die Kompatibilitätsprobleme unterschiedlicher Marken innerhalb der USA behoben, doch der Computer wurde zu einem internationalen Phänomen und allein die Betrachtung der Buchstaben führt zu Unterschieden, da nicht jede Sprache das gleiche Alphabet verwendet (man denke nur etwa an die arabischen Schriftzeichen oder das kyrillische Alphabet der östlichen Sprachen, ganz abgesehen von den fernöstlichen Schriftzeichen der Chinesen und Japaner). Der amerikanische Standard reichte also nicht mehr aus. Nach mehreren Jahren der Entwicklung erschien 1991 schließlich die erste, noch sehr unvollständige, Version des Unicode. Der Unicode wird dauerhaft erweitert. Die aktuelle Version erschien im April 2008. Der Unicode war ursprünglich ein 16-bit Code, was eine Codierung von 65.536 Zeichen ermöglichte, doch mit dieser Anzahl stieß man schon bald an die Grenzen. Diese Kapazität genügt zwar zur Codierung der Buchstaben der meisten Sprachen, doch sie genügt nicht zur Codierung sämtlicher Sonderzeichen. Also wurde der Zeichensatz erweitert, sodass heute im Unicode 17 Bereiche zu jeweils 65.536 Zeichen zum Einsatz kommen. Mit dieser Erweiterung lassen sich schließlich über eine Million Zeichen Codieren. Man geht davon aus, dass diese Zeichenmenge zur Codierung aller bekannten Zeichen genügt. Die aktuelle Version benötigt mit etwas über 100.000 Zeichen nur etwa ein

Zehntel dieser Kapazität, doch wie bereits erwähnt wird der Unicode ja dauerhaft erweitert. Aus Platzmangel wird hier auf eine Darstellung der im Unicode festgelegten Zeichen verzichtet.[196]

7. Huffman-Code

Computer und Internetzugänge via Breitbandverbindung werden zwar immer schneller, dennoch sind Kapazitäten und Übertragungsraten begrenzt. Das Zauberwort hierfür lautet Kompression. Ein Beispiel für Datenkompression mittels Codierung ist der 1952 von David Huffman entwickelte Huffman-Code. Beim Huffman-Code wird gezielt nach Unterschieden in der Häufigkeit des Auftretens von Zeichen gesucht. Während ASCII-Zeichen normalerweise in einer 7-bit Folge codiert werden, erfolgt die Codierung nach Huffman bei einem Bit beginnend und aufsteigend, wobei häufige Zeichen kürzere Codes bekommen und seltenere Zeichen längere Codes. Der Vorgang bei der Erstellung des Huffman-Codes führt nachweislich stets zur optimalen Codierung, was die Speichergröße betrifft.
Betrachten wir das Wort Ananas. Der erste Schritt im Huffman-Code sieht zunächst vor die einzelnen Zeichen zu trennen und eine Häufigkeitsanalyse durchzuführen. Bei unserem Beispiel taucht der Buchstabe A dreimal auf, der Buchstabe N zweimal und der Buchstabe S einmal. Dabei wird für jeden Buchstaben ein eigener Baum erstellt in dessen Wurzel die Buchstabenhäufigkeit steht und an dessen Blatt der Buchstabe steht.

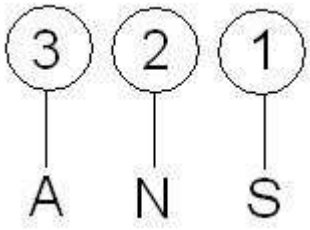


Abbildung 5.7

Der Huffman-Code beginnt nun mit den beiden am seltensten vorkommenden Zeichen (in unserem Fall also N und S) und fügt sie zu einem Baumdiagramm zusammen, dessen Wurzel als Wert die Summe der Häufigkeit der beiden Buchstaben besitzt (oder allgemeiner: die Summe aller Buchstaben in diesem Baum, doch im ersten Schritt sind dies ja gerade immer nur zwei Buchstaben).

[196] http://de.wikipedia.org/wiki/Unicode, letzter Zugriff: 15.04.2009

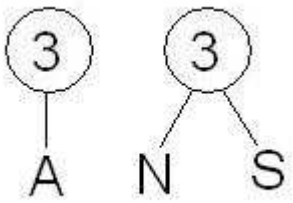


Abbildung 5.8

Nun fährt man mit dem System fort. Es werden wieder die beiden Bäume mit den kleinsten Häufigkeiten gesucht und zu einem neuen Baum zusammengefügt. Nach diesem Schema entsteht schließlich der Huffman-Baum. In unserem Beispiel ist hier allerdings schon Schluss.

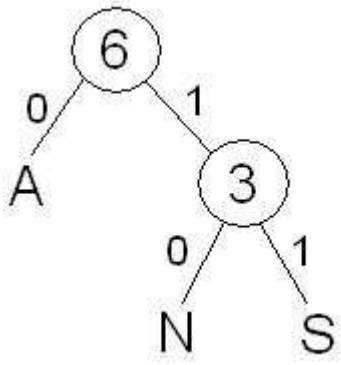


Abbildung 5.9

Nun kann man die Codierung für die einzelnen Zeichen an den Ästen des Baumes ablesen. Dabei fällt sofort auf, dass die Bitfolge der Zeichen deutlich geringer ist als beim ASCII-Code. Während der Buchstabe A dort 7-bit belegt, benötigt er jetzt nur noch 1-bit und auch die beiden anderen Buchstaben brauchen nur noch 2-bit. Diese Technik kommt insbesondere als verlustfreie Komponente verlustbehafteter Datenkompressionsverfahren zum Einsatz, beispielsweise beim vielfach verwendeten Abspeichern eines Bildes im .jpg-Format. Hier werden allerdings keine Buchstaben oder Zeichen codiert, sondern Pixelfolgen.

8. EAN und ISBN

EAN ist die Abkürzung für Europäische Artikelnummer. Mittlerweile wird sie auch als Internationale Artikelnummer bezeichnet, da sie von vielen außereuropäischen Ländern adaptiert wurde. Sie wird zur Kennzeichnung von Produkten, die verkauft werden, verwendet.

Aufbau der EAN:

Länderkennung (2 Ziffern) Herstellernummer (5 Ziffern) Artikelnummer (5 Ziffern) Prüfziffer (1 Ziffer)

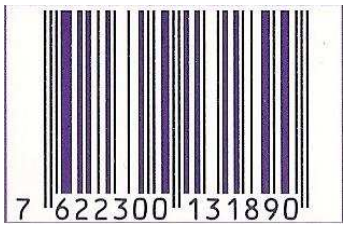


Abbildung 5.10

Die Länderkennung wird International vergeben. Die Zahlen 40 bis 44 stehen beispielsweise für Deutschland. Die 5-ziffrige Herstellernummer wird dann national vergeben. Die Artikelnummer vergibt der Hersteller. Die Prüfziffer am Ende der EAN dient dazu Fehler in der EAN zu finden. Sie wird berechnet, indem man die Summe aller vorangegangenen Ziffern bestimmt, wobei jede zweite Ziffer mit drei multipliziert wird. Die letzte Ziffer der Summe wird von 10 subtrahiert. Das Ergebnis ist die Prüfziffer. In dem Fall, dass die letzte Ziffer der Summe eine Null ist und die Prüfziffer damit 10 wäre, wird sie 0 gesetzt.[197]

In der folgenden Gleichung zeigt der Index an der Variablen p die Position der Ziffer in der EAN an:

$p_{13} = 10 - ((p_1 + 3*p_2 + p_3 + 3*p_4 + p_5 + 3*p_6 + p_7 + 3*p_8 + p_9 + 3*p_{10} + p_{11} + 3*p_{12}) \mod 10)$

Klammert man die 3 in dieser Gleichung aus, so ergibt sich:

$p_{13} = 10 - ((p_1 + p_3 + p_5 + p_7 + p_9 + p_{11} + 3*(p_2 + p_4 + p_6 + p_8 + p_{10} + p_{12})) \mod 10)$

Möchte man die Regel berücksichtigen, dass das Ergebnis 10 auf 0 gesetzt wird, so kann man die gesamte rechte Seite in Klammern setzen und mod 10 rechnen, denn wäre das Ergebnis zu diesem Zeitpunkt eine Ziffer zwischen null und neun, so würde mod 10 gerade nichts verändern. 10 mod 10 hingegen ist gleich 0. Die Gleichung lautet dann also:

$p_{13} = (10 - ((p_1 + p_3 + p_5 + p_7 + p_9 + p_{11} + 3*(p_2 + p_4 + p_6 + p_8 + p_{10} + p_{12})) \mod 10)) \mod 10$

Eine falsche Ziffer führt also zu einer anderen Summe und damit einer falschen Prüfziffer. Durch die Verdreifachung des Wertes an jeder zweiten Position, können Zahlendreher ausgeschlossen werden. Allerdings fällt auch auf, dass mehrere Fehler an unterschiedlichen Stellen sich ausgleichen können, sodass die Prüfziffer nicht verfälscht wird und das System den Fehler damit nicht bemerkt. Eine Vertauschung

[197] http://de.wikipedia.org/wiki/European_Article_Number, letzter Zugriff: 15.04.2009.

direkt benachbarter Zahlen lässt sich in der Regel erkennen, solange es sich nicht um die gleichen Ziffern handelt. Sind es allerdings die gleichen Ziffern, dann spielt eine Vertauschung ohnehin keine Rolle, da sich ja am Code nichts ändert.

Die ISBN ist die internationale Standartbuchnummer (International Standard Book Number). Wie der Name schon sagt, lassen sich mit der ISBN Bücher weltweit eindeutig kennzeichnen. Dies wurde im Zuge der Globalisierung wichtig um beispielsweise bei einer Bestellung eines ausländischen Buches dieses auch korrekt identifizieren zu können. Die Nummer war zunächst 10-stellig. Zur Angleichung an die 13-stellige internationale Artikelnummer EAN und weil man langsam an die Kapazitätsgrenzen geriet, wurde die ISBN im Jahre 2006 auf 13 Stellen erweitert. Wie auf dem folgenden Bild gut zu sehen ist, sind bei Büchern ISBN und EAN identisch (Die Form gibt die ISBN vor und nicht die EAN)

Abbildung 5.11

Der grundsätzliche Aufbau der ISBN ist:

ISBN Präfix – Ländernummer – Verlagsnummer – Titelnummer – Prüfziffer

Für das Beispiel bedeutet das also:

Präfix: 978

Ländernummer: 3

Verlagsnummer: 8171

Titelnummer: 1814

Prüfziffer: 4

Das Präfix wurde erst mit der 13-stelligen ISBN eingeführt und lautete zunächst für alle Bücher 978. Seit 2008 gibt es auch 979 als Präfix. Die Ländernummer wird von der internationalen ISBN-Agentur festgelegt. Die uns vorliegende Nummer 3 identifiziert das Buch als ein aus dem deutschsprachigen Raum stammendes Werk. Die Verlagsnummer wird dem entsprechenden Verlag von der regionalen ISBN-Agentur zugewiesen. Die Titelnummer bestimmt der Verlag schließlich selbst. Die Prüfziffer berechnet sich ebenso wie bei der EAN.[198]

[198] http://de.wikipedia.org/wiki/Internationale_Standardbuchnummer, letzter Zugriff: 15.04.2009.

VI. Die Unterrichtseinheit

1. Didaktische Überlegungen

Zu Beginn der Planungsphase einer Unterrichtseinheit müssen gewisse methodisch-didaktische Überlegungen angestellt werden. Diese dienen zwar in erster Linie den einzelnen Stunden selbst, allerdings muss sich bereits die Auswahl der Stunden an solchen Überlegungen messen lassen. Zu solchen Überlegungen zählen die Lerntheorien.
Theorien dazu wie Menschen lernen gibt es unzählig viele. Die wohl am weitesten verbreiteten lassen sich in drei Gruppen einteilen: Die behavioristisch, die kognitivistisch und die konstruktivistisch geprägten Lerntheorien.

1.1. Behavioristisch geprägte Lerntheorien[199]

Der Begriff Behaviorismus leitet sich aus dem Englischen von „to behave“ ab (to behave = sich benehmen, betragen, verhalten, …). Der Behaviorismus betrachtet sämtliche Verhaltensformen als Reaktion auf einen zuvor gegebenen Reiz, wobei diese Reiz-Reaktionen erlernt werden können. Der Vorgang des Erlernens bezieht sich hierbei auf die klassische Konditionierung, wie sie etwa von Pawlows Hunden bekannt ist.
Während die ersten behavioristischen Ansätze das Reiz-Reaktions-Verhalten auf äußerliche physische Reize und damit die klassische Konditionierung beschränkten, erweiterte Burrhus Frederic Skinner das Konzept um die operante Konditionierung. Bei der operanten Konditionierung wirkt der Mensch auf seine Umwelt ein, dies gibt ihm Entscheidungsmöglichkeiten. Jede Entscheidung führt dann aber zu einer Reaktion, aus der das Individuum selbst lernt. Diese Reaktionen können beim Individuum zu einer Verstärkung erwünschten Verhaltens führen, oder zu einer Bestrafung unerwünschten Verhaltens. Ein solcher Verstärker bildet zusammen mit den Umständen, der zu ihm geführt hat, schließlich den Reiz.
Die Kritik an Skinner richtet sich eher gegen die Anwendung des Prinzips als gegen seine These selbst, da die Kritiker befürchten, man könne es ausnutzen, um das menschliche Verhalten zu kontrollieren.

[199] Baumgart, Franzjörg: Entwicklungs- und Lerntheorien, S. 109 ff.

Für den Unterrichtet bedeutet dieser Ansatz besonders die aufmerksame Abwägung solcher Reize. Der Lehrer muss sich die Frage stellen, ob durch seinen Unterricht Reize ausgelöst und damit Reaktionen verknüpft werden. Eine solche Abwägung ist insbesondere daher wichtig, weil die im Schüler ausgelösten Reaktionen sowohl positiv als auch negativ sein können.

1.2. Kognitivistisch geprägte Lerntheorien[200]

Bei der kognitivistischen Lehre ist die Reaktion nicht zwingend mit dem Reiz verbunden. Vielmehr setzt sich das Individuum in seinen Denkprozessen mit dem Reiz und der Umwelt auseinander und reagiert erst anschließend. Lernen geschieht in diesem Sinne durch die kognitive Auseinandersetzung mit der Materie (es gilt diesbezüglich als Informationsverarbeitungsprozess im Gehirn), wobei die Denkprozesse nicht nur das Verhalten verändern, sondern gleichzeitig auch die kognitiven Fähigkeiten.
Als Begründer der kognitiven Lerntheorien gilt Jean Piaget. Piaget unterscheidet in seinen Lehren zwischen Akkommodation und Assimilation. Er geht davon aus, dass es gewisse Einheiten in der kognitiven Struktur des Menschen gibt, die er als Schema bezeichnet. Die kognitive Struktur ist dabei die Gesamtheit aller kognitiven Fähigkeiten, die dem Mensch zum Lösen einer bestimmten Situation zur Verfügung stehen. Die Assimilation ist nun die Anwendung eines Schemas auf den Einzelfall, wodurch die Situation bewältigt wird. Tritt eine Situation auf, für deren Lösung kein passendes Schema vorhanden ist, so findet die Akkommodation statt. Mit Hilfe kognitiver Fähigkeiten wird ein bereits bestehendes Schema so verändert, dass es auf den neu eingetretenen Fall passt und im Sinne der Assimilation angewendet werden kann.
Der Kognitivismus konnte aber ebenfalls nicht die Auffassung der äußerlichen Steuerung, wie sie der Behaviorismus prägte, ausräumen.

[200] Buth, Manfred: Lerntheorien, S. 45 ff.

1.3. Konstruktivistisch geprägte Lerntheorien[201]

Der im Laufe der 90er Jahre aufkommende Konstruktivismus sieht den Lernvorgang nun nicht mehr in der Wissensübertragung vom Lehrenden zum Lernenden, sondern als eigener Konstruktionsprozess beim Lernenden, der stark durch Handlung und Erfahrung geprägt ist. Wissen wird im konstruktivistischen Ansatz nicht mehr als Gut angesehen, welches weitergegeben werden kann. Das Wissen kann damit nicht mehr vom lernenden Individuum und der zugehörigen Lernsituation abgekoppelt werden.
Die Ausprägungen konstruktivistischer Ansätze reichen dabei von autonomen Konstruktionshandlungen des einzelnen Individuums bis hin zu gemeinschaftlichen Prozessen in Gruppen von Lehrendem und Lernendem, wenngleich Letzteren vorgeworfen wird, dass sie dem Grundsatz des Zusammenhangs zwischen Wissen, Individuum und Lernsituation nicht ganz gerecht werden.
Die konstruktivistischen Lerntheorien lehnen die Steuerbarkeit des Individuums durch äußere Impulse nun schließlich ab, sie stellen das Subjekt in den Mittelpunkt des Geschehens und fordern eine reichhaltige Lernsituation.

2. Rahmenbedingungen

Unterricht hängt neben den individuellen Bedingungen auch immer in direkter Weise von den allgemeinen Rahmenbedingungen ab. Im Folgenden sollen diese äußeren Bedingungen aufgezeigt werden.

2.1. Die Anne-Frank-Schule

Die Anne-Frank-Schule liegt im Karlsruher Stadtteil Oberreut. Es handelt sich dabei um eine kombinierte Grund- und Hauptschule mit angeschlossener Werkrealschule, außerdem wird in Zusammenarbeit mit dem nahe gelegenen Kinderhort eine Nachmittagsbetreuung angeboten. Die Schule selbst ist umgeben von mehrstöckigen Wohnhäusern. Oberreut gilt innerhalb Karlsruhes als ein sozialer Brennpunkt, da der Anteil an Immigranten überdurchschnittlich ist.

[201] Arnold, Patricia: Einsatz digitaler Medien in der Hochschullehre aus lerntheoretischer Sicht, S. 4.

2.2. Die Klasse 4d

Ich führe meine Einheit in der Klasse 4d durch. Die Lehrerin Frau Blume unterrichtet die Schüler bereits seit dem Schuleintritt als Klassenlehrerin. Die Klasse besteht insgesamt aus 22 Schülern, 12 Mädchen und 10 Jungen. Obwohl ein Großteil der Schüler Eltern mit Migrationshintergrund haben, sind die Schüler selbst alle deutsche Staatsbürger. Laut Aussage der Lehrerin macht sich das Oberreuter Umfeld in dieser Klasse nicht allzu sehr bemerkbar. Frau Blume war so freundlich mir einen Zeitrahmen von zwei Wochen für die Einheit in ihrer Klasse einzuräumen. Ich habe sie angefragt, weil ich in dieser Klasse bereits zwei Schulpraktika absolviert habe und daher sowohl die Lehrerin, als auch die Schüler kenne. Ich bin davon überzeugt, dass die Schülerinnen und Schüler in der Lage sind, die Inhalte, die ich ausgewählt habe, aufzunehmen, zu verstehen und auch den inneren Zusammenhang zu erkennen.

3. Themenauswahl

Die Themenauswahl muss, dem genetischen Prinzip entsprechend, exemplarisch erfolgen. Eine umfassende Betrachtung der gesamten Genese der Kryptologie ist rein zeittechnisch im Schulunterricht nicht möglich, darüber hinaus verliert auch das interessanteste Thema irgendwann an Reiz und damit auch an Motivationskraft. Die Auswahl der einzelnen Themen aus dem Gesamtkanon der Kryptologie ist jedem selbst überlassen, allerdings sollte man einige Grundbedingungen beachten: Exemplarisch bedeutet nicht nur, dass man irgendein Beispiel wählt, dieses sollte auch einen Beispielcharakter aufweisen. Wenn ich also vor einiger Zeit die Verfahren grob kategorisiert habe (in Transpositionen, monoalphabetische und polyalphabetische Substitutionen, symmetrische und asymmetrische Verfahren, ...) dann wäre es durchaus sinnvoll beispielhafte Vertreter dieser Gruppen auszuwählen, wobei man den Entwicklungsstand der Schüler nicht aus dem Fokus verlieren darf. Hier wäre etwa anzubringen, dass Schülern im Grundschulalter sowohl die mathematischen Voraussetzungen als auch das Abstraktionsvermögen für das asymmetrische RSA-Verfahren fehlen. Dass dieses Verfahren von Schülern höheren Alters hingegen sehr gut verstanden werden kann, hat Herr Stefan Kuchenbrod in

seiner wissenschaftlichen Hausarbeit bereits aufgezeigt.[202] Eine weitere Grundüberlegung folgt dem genetischen Aspekt, weshalb ich die genetische Vorgehensweise bei der Vermittlung kryptographischer Verfahren sehr schätze. Aus Problemen und Unzulänglichkeiten einzelner Verfahren, begaben sich nicht nur die Menschen in der Geschichte auf die Suche nach neuen Methoden, es ergibt sich auch für unsere Schüler der Anreiz „bessere“ oder sicherere Verfahren kennen zu lernen. Darüber hinaus können die Schüler dann bereits auf ihr Vorwissen bei vorangegangenen Verfahren aufbauen. Man kommt dann vom Einfachen zum Schwierigeren, Komplizierteren oder Abstrakteren. Frau Blume war so freundlich mir für die Einheit in ihrer Klasse sechs Stunden einzuräumen. Ich möchte im Folgenden meine Themenauswahl vorstellen und in einigen Sätzen erklären, wieso ich mich ausgerechnet für diese Themen entschieden habe:

1. Stunde: Skytale von Sparta
2. Stunde: Caesar-Verfahren
3. Stunde: Vigenère-Verfahren
4. Stunde: Fleissner-Methode
5. Stunde: Problem der Schlüsselverteilung
6. Stunde: Steganografische Methoden

Ursprünglich hatte ich sieben Stunden eingeplant. Die weitere Stunde sollte den Codierungsaspekt von Geheimschriften zeigen und enthielt die Behandlung der Braille-Schrift (sowie gegebenenfalls des Morse-Code). Aus Zeitgründen wurde aber eine Stunde gestrichen und ich habe mich nach langem Überlegen dazu durchgerungen diese Stunde zu streichen, wenngleich der Codierungsaspekt in der Unterrichtseinheit jetzt ganz außen vor gelassen wird. Der Grund dafür ist, dass die Lehrerin meinte der Morse-Code wäre für den Wissensstand der Viertklässler schon zu gering und meine Überlegung, dass der Codierungsaspekt für die Grundschule wahrscheinlich zu wenig hergäbe. Diese Überlegung kommt daher, dass der Codierungsaspekt heute insbesondere in der Informationstechnik wichtig ist, den Schülern der vierten Klasse allerdings die informationstechnischen Grundlagen fehlen um die Verfahren dieses Bereiches zu verstehen.

[202] vgl. Stefan Kuchenbrod: Moderne kryptographische Verfahren im Mathematikunterricht der Sekundarstufe am Beispiel der RSA-Verschlüsselung.

3.1. Skytale von Sparta

Die Skytale von Sparta ist nicht nur eines der ältesten uns bekannten kryptographischen Verfahren, sie ist auch eine absolut klassische Transpositionsmethode. Das erkennt man unter anderem daran, dass sie in fast jedem Buch über Kryptographie Erwähnung findet. Sie eignet sich hervorragend für den Schulunterricht, da das Verfahren selbst relativ einfach auszuführen ist und die nötigen Mittel nicht allzu kostenintensiv, sowie leicht herzustellen sind. Trotz ihrer Einfachheit bietet sie allerdings einige Stolpersteine (unterschiedlicher Umfang, falsch herum wickeln, an der falschen Seite anfangen, ...), die den Schülerinnen und Schülern aufzeigen, dass sie sorgfältig arbeiten müssen. Da sich die Materialien auch sehr gut zuhause vorbereiten lassen, kann man den Schülern bereits fertige Botschaften vorlegen, die sie nicht lesen können. Das weckt den „Rätselinstinkt“ und die Schüler sind umgehend motiviert die Nachricht herauszufinden. Außerdem zeigen die Abhandlungen in den einschlägigen kryptographischen Werken, dass die Spartaner die Verschlüsselung der Skytale mit einem steganografischen Verfahren (Verwendung des Bandes als Gürtel) kombinierten, sodass sich auch dieser Bereich anschneiden lässt. Sie hat allerdings ein schwerwiegendes Problem: Es genügt die einfache Kenntnis darüber, dass die Methode der Skytale verwendet wurde, um in einer absehbaren Zeit die einfache Verschiebung nachzubilden und den Geheimtext somit sichtbar zu machen. Aus dieser Problematik heraus ergibt sich die Frage nach einem Verfahren, welches auf eine solch einfache Buchstabenverschiebung verzichtet.

3.2. Das Caesar-Verfahren

Hier kommt das Caesar-Verfahren ins Spiel. Die Caesar-Verschiebung ist, im klassischen Kontrast zur Transpositionschiffre Skytale, eine monoalphabetische Substitution. Die Buchstaben werden hier also ersetzt. Hier kommt man durch eine einfache Verschiebung der Buchstaben nicht mehr zu einer sinnvollen Lösung (außer es handelt sich um einen bösen Ausnahmefall). Das Caesar-Verfahren ist wohl die bekannteste monoalphabetische Substitution. Dass sie für den Einsatz in der Grundschule geeignet ist, zeigen gleich mehrere Aufsätze zu diesem Thema in Grundschulzeitschriften. Die Geeignetheit dieses Verfahrens für den Einsatz in der

Grundschule ergibt sich aus mehreren Gründen. Zum Einen ist dieses Verfahren untrennbar mit dem Namen einer großen historischen Persönlichkeit verbunden, nämlich Julius Caesar, dessen Namen selbst die meisten unserer Grundschüler schon einmal gehört haben, zum Anderen basiert das Caesar-Verfahren auf der elementarsten unserer Rechenmethoden: die einfache Addition die wir bereits in Klasse 1 vermitteln (bei einer Verschiebung um drei Stellen rechnet man „+3“). Damit sind sämtliche Grundlagen für den Einsatz gelegt. Eine Caesarscheibe können die Schüler selbst mit einfachsten und kostengünstigen Mitteln herstellen, dadurch erhalten wir wiederum eine starke Handlungsorientierung und die Schüler können sich mit dem von ihnen hergestellten Werk identifizieren. Schließlich bietet die Caesar-Methode auch noch einige weitere interessante Möglichkeiten. Beschriftet man nur eine der beiden Scheiben im Vorfeld und überlässt die Beschriftung der zweiten Scheibe den Schülern, so können sie selbst entdeckend tätig werden: Denkbar wäre hier, dass die Schüler feststellen, dass jeder Buchstabe des Alphabets vorkommen muss, dass entsprechend auch jeder Buchstabe nur einmal vorkommen darf und schließlich auch, dass sie nicht in der Reihenfolge auftreten müssen. Die Caesar-Methode bietet also vielfältige Möglichkeiten. Dennoch können die Schülerinnen und Schüler erfahren, dass sie leider unsicher ist, nachdem zunächst arabische Gelehrte entdeckten, dass jede Schrift ihre Buchstaben unterschiedlich oft verwendet und daraufhin die Häufigkeitsanalyse von Buchstaben einführten mit der sie die monoalphabetischen Verschlüsselungen knackten. Zeigt man den Schülern dieses Problem auf, indem man sie einen Text selbst mit Hilfe der Häufigkeitsanalyse knacken lässt, dann liegt es nahe den Schülerinnen und Schülern im nächsten Schritt eine Methode vorzustellen, die dieser Analyse widersteht.

3.3. Vigenère-Verfahren

Genau an dieser Stelle setzen die polyalphabetischen Verschlüsselungen an. Das klassische Verfahren schlechthin ist hier das Vigenère-Verfahren. Diese Methode stellt für die Schüler schon eine kleine Hürde dar, doch wenn es ihnen gelingt das Verfahren zu durchdringen, dann haben sie eine Methode an der Hand, die heutzutage zwar auch nicht mehr sicher ist, allerdings von Laien im Gebiet der Kryptographie kaum geknackt werden kann. Für den Einsatz in der Grundschule würde ich das Vigenère-Verfahren als obere Grenze setzen. Wird es noch

komplizierter, dann eröffnet sich die Methode hinter der Geheimschrift nur einem so kleinen Anteil der Schülerinnen und Schüler und die Übrigen bleiben auf der Strecke, dass es kaum noch Sinn macht. Um das Vigenère-Verfahren im Unterricht behandeln zu können bedarf es aber eines großen Maßes an Vorbereitung, denn in der Grundschule ist es absolut unsinnig zu glauben, die Schüler könnten dieses Verfahren verstehen, indem man es ihnen zeigt und erklärt. Die Schüler müssen es ausprobieren und anwenden können, ansonsten wird schon bei dieser Methode das Verständnis ausbleiben. Die Schülerhandlung darf auch hier nicht zu kurz kommen. Nun bietet die Vigenère-Verschlüsselung leider nicht die Möglichkeit Tafeln selbst schnell herzustellen, wie das bei Skytale und Caesarscheibe der Fall war. Die Handlung der Schüler beschränkt sich hier also hauptsächlich auf die Durchführung des Verfahrens. Und damit steht der Lehrer vor einem Problem. Für eben diese Durchführung benötigen die Schüler Vigenère-Tafeln um die polyalphabetische Verschlüsselung durchzuführen. Diese muss der Lehrer aber bereits im Vorfeld angefertigt haben (mit viel Glück kann er diese Aufgabe an die Werkrealschule abgeben, ansonsten muss er selbst Hand anlegen). Meine Prüfer waren so freundlich mich mit den Materialien der PH Karlsruhe zu versorgen. Dort liegen 19 Tafeln bereit (die Verwendungsweise erkläre ich im Abschnitt zur praktischen Umsetzung und Reflexion der Stunde selbst). Um jedem Schüler eine eigene Tafel zukommen zu lassen, habe ich sechs solcher Tafeln neu angefertigt. Die Arbeitszeit dafür lag bei etwa 4 Stunden und 30 Minuten. Die PH Karlsruhe hat nun einen Satz von Tafeln, der für die meisten Klassen ausreichen dürfte. Wenn man aber als Lehrer auf diese Materialien nicht zurückgreifen kann, dann heißt es entweder sich eine weniger aufwendige Variante zu überlegen, oder diese Stunde weit im Voraus zu planen um genügend Zeit zur Herstellung der Tafeln zu haben.

3.4. Fleissner-Methode

Die Fleissner-Methode stellt wieder eine Transpositionschiffre dar. Ich habe zwar bereits mit der Skytale ein Verschiebeverfahren eingeplant, dennoch halte ich es für durchaus sinnvoll das Fleissner-Verfahren zusätzlich zu behandeln. Die Methode nach Fleissner funktioniert nämlich mit Hilfe einer Schablone, die mehrmals gedreht wird, sodass man an diesem Verfahren sehr schön erkennen kann, dass sich nicht nur die Arithmetik zu Verschlüsselungen eignet, sondern auch die Geometrie. Damit

hat das Fleissner-Verfahren einen Platz in einer kryptographischen Unterrichtseinheit verdient. Hinzu kommt, dass die Schüler sich hier ihre Schablonen wieder selbst herstellen können und sich dabei Überlegungen zur Symmetrie machen müssen oder ihnen hoffentlich im Nachhinein Bedingungen für die Funktion dieses Verfahrens bewusst werden. In meinem Aufbau lassen sich zu diesem Zeitpunkt Analogien und Unterschiede zur Skytale erkennen (sowie zu den beiden Substitutionsverfahren), die deutlich machen wie vielfältig die Kryptographie sein kann, obwohl das zugrunde liegende Verfahren (Transposition) doch gleich geblieben ist. Allein daher halte ich es schon für sinnvoll, wenigstens von einer Methode mindestens zwei unterschiedliche Verfahren aufzuzeigen, die sich in ihrer Verwendung stark unterscheiden. Ich hatte überlegt die beiden Transpositionschiffren nacheinander zu behandeln, allerdings wollte ich den Aufbau über die Problematiken des einen Verfahrens hin zum nächsten Verfahren nicht unterbrechen, außerdem glaube ich, dass die Schüler nach der Behandlung des Vigenère-Verfahrens etwas verdient haben, das wieder stärker handlungsorientiert ist und diese Möglichkeiten bietet die Herstellung der Fleissner-Schablone allemal, zumal sich die Schüler hier sogar mehrere unterschiedliche Schablonen herstellen und verwenden können.

3.5. Das Problem der Schlüsselverteilung

Das Problem der Schlüsselverteilung habe ich ausgewählt, weil es einerseits das klassische Problem der (symmetrischen) Kryptographie schlechthin darstellt und ich finde, dass man auch Schülern dieses Problem deutlich machen sollte und weil ich andererseits die Schüler fordern wollte. Eine wissenschaftliche Hausarbeit soll ja auch immer einen forschenden Inhalt darstellen und so wollte ich in meiner Unterrichtseinheit die Grenzen des Verständnisses von Grundschülern immer wieder austesten. Ich denke, dass sich dieses Problem dafür eignet. Das Problem selbst ist auch offenkundig und stellt sich nach der Behandlung von vier symmetrischen Verfahren dem interessierten Teilnehmer praktisch von selbst, die Lösung (Diffie-Hellman-Verfahren) hingegen ist relativ abstrakt, sodass ich von Anfang an nicht vorgehabt hatte eine Lösung für dieses Problem vorzustellen, bis ich bei Simon Singh las, wie er die mathematischen Einwegfunktionen mit Hilfe von Farben analog erklärt. Ich glaube, dass diese Erklärung auch von Schülern verstanden werden kann. Wenn dem aber so ist, dann kann es eigentlich keinen Grund geben, weshalb

man dieses Problem und seine Lösung den Schülern nicht zugänglich macht (insbesondere dann, wenn man aufgrund der zu hohen Komplexität keine asymmetrischen Verfahren durchnimmt und die Schüler daher keine Möglichkeit haben dieses Problem anderweitig zu umgehen.)

3.6. Steganografische Methoden

Meine Arbeit und auch die Unterrichtseinheit widmen sich in erster Linie der Kryptographie. Das kommt daher, dass diese Methoden heute meist wichtiger sind als steganografische Verfahren und dass die kryptographischen Verfahren selbst oftmals auf mathematischen Grundlagen beruhen und ich diese Arbeit im Fach Mathematik, bzw. im mathematisch-naturwissenschaftlichen Fächerverbund, schreibe. Steganografische Methoden hingegen beruhen eher selten auf der Mathematik, zumindest wenn man außer Acht lässt, dass die digitale Steganografie den Computer verwendet und dieser stark mathematisch geprägt ist. Dennoch gehört auch die Steganografie zur Kryptologie und sie bietet einen schönen Kontrast zur Kryptographie, da sie einen ganz anderen Weg einschlägt um die Nachrichten geheim zu halten, einen Weg, der den Schülern wahrscheinlich sogar nahe liegender erscheint als die Verschlüsselung, das Verstecken. Ich habe diesen Punkt, oder diese Stunde, mit „steganografische Methoden“ überschrieben, da es mir ein Anliegen war den Schülern, zur besseren Unterscheidung und Verdeutlichung der Unterschiede, gleich mehrere Methoden aufzuzeigen. Die Positionierung dieser Stunde am Ende der Einheit erfolgte aus zwei Gesichtspunkten: Erstens wollte ich sie vom Rest deutlich abtrennen, um den Unterschied zwischen den Methoden deutlich zu machen und das Behandeln in der Mitte der Einheit würde zu Verwirrungen führen. Zum Zweiten steht im Zentrum dieser Stunde das Verwenden von unsichtbarer Tinte, die mit Feuer wieder sichtbar gemacht wird, sodass sich diese Stunde hervorragend als fulminantes Finale anbietet.

4. Praktische Umsetzung der Stunden

Der folgende Teil befasst sich mit der praktischen Umsetzung der einzelnen Unterrichtsstunden. Sämtliche von mir verwendeten Materialien, Bilder, die ich während der Stunden gemacht habe, sowie die entsprechenden Unterrichtsskizzen befinden sich im Anhang zu dieser Arbeit.

4.1. Skytale von Sparta

Da die Stunde, in der ich die Skytale besprechen möchte, auch noch den Einstieg in die gesamte Einheit bildet, habe ich mir überlegt, den Schülern eine verschlossene Schatztruhe mitzubringen in der sich eine Skytale sowie eine dazugehörige, vorher vorbereitete, geheime Botschaft befindet. Ich erhoffe mir dadurch den Reiz an Geheimnissen und Schätzen anzusprechen und damit von Beginn an ein hohes Motivationspotential zu schaffen. Für den Beginn habe ich mir überlegt die Schüler im Stuhlkreis zusammenkommen zu lassen. Einerseits haben die Schüler damit alle einen guten Blick auf das, was in der Mitte passiert und sie sind näher am Geschehen, andererseits hat der Kreis selbst die Bedeutung einer verschworenen Gemeinschaft, sodass die Bedeutung von Geheimnissen und Schätzen hier noch einmal unterstrichen wird. Ich erhoffe mir, dass die verschlossene Schatzkiste bereits die Neugierde der Schüler weckt, wenn sie erst einmal offen ist und die Schüler mit Erstaunen auf etwas blicken, was einerseits einen Schatz darstellen soll, ihnen andererseits aber überhaupt nichts sagt (die Skytale und das Band), dann müssten sie relativ schnell darauf kommen, dass es sich um eine ganz geheime Nachricht handelt und sie sollten probieren diese zu entziffern. Den Einstieg hätte man alternativ auch als Rollenspiel planen können, indem man eine Nachricht wirklich überbringen lässt und gleich an dieser Stelle auf die Gefahren hinweist, ich fürchte allerdings, dass eine solche Herangehensweise in einem Chaos ausartet, wenn einzelne Schüler übereinander herfallen um sich die Nachricht aus den Händen zu reißen. Bindet man hingegen nur einen kleinen Teil der Schüler ein, so besteht die Gefahr, dass die anderen Schüler sich benachteiligt fühlen oder ihr Interesse anderen Dingen widmen. Daher habe ich mich für diesen Einstieg entschieden. Im nächsten Schritt sollen die Schüler im Gespräch mit der Gruppe den Zusammenhang zwischen der Kiste und ihrem persönlichen Leben erkennen. Indem wir uns darüber

klar werden, dass auch jeder von uns Geheimnisse besitzt, die es zu schützen gilt, bemerken die Schüler hoffentlich, die Wichtigkeit des Einsatzes solcher Verschlüsselungsmethoden. Ich schätze, dass mindestens ein Schüler oder eine Schülerin ein Tagebuch führt, oder schon einmal eines gesehen hat, sodass er oder sie weiß, dass man solche Bücher zusperren kann und wieso man das macht. Da es sich um die erste Stunde handelt, müssen einige Grundbegriffe erläutert werden. Dies sind insbesondere die Begriffe „verschlüsseln“, „entschlüsseln“ und „Schlüssel“. Diese Begriffe plane ich analog über die, mit einem Vorhängeschloss versperrte, Kiste zu erklären. Nach einer genaueren Betrachtung des Verfahrens mittels der Skytale gehen die Schülerinnen und Schüler dann an ihre Plätze zurück, wo sie sich in Partnerarbeit gegenseitig verschlüsselte Texte schreiben. Zu diesem Zweck bekommt jede Schülerin und jeder Schüler ein ca. 20cm langes Stück Isolationsrohr. Auf diesem Schaumstoffrohr lässt sich mit Pinnadeln relativ leicht ein Stoffstreifen aufziehen, der sich anschließend problemlos beschreiben lässt. Da jeder Schüler ein solches Stück Rohr, sowie einen Stoffstreifen und einen Stift erhält, können alle Schüler gleichzeitig arbeiten.
Das Hauptziel der Stunde ist, dass die Schülerinnen und Schüler erkennen, dass jeder Mensch Geheimnisse besitzt, die er schützen will und muss und dass Geheimschriften Möglichkeiten bieten dieses Ziel zu erreichen. Außerdem kennen sie ein kryptographisches Verfahren, nämlich die Skytale von Sparta.
Nebenbei lernen sie auch noch die grundlegenden Begriffe „verschlüsseln“, „entschlüsseln“ und „Schlüssel“ kennen, außerdem wissen sie, dass Geheimschriften schon seit der Antike verwendet werden und sie kennen Probleme des Verfahrens, welches sie kennen gelernt haben. Solche Probleme wären z.B. die Angreifbarkeit des Verfahrens mittels Brute Force Methode, da man bei Kenntnis des Verfahrens die Verschiebung und einer endlichen Anzahl von Schritten durchprobieren kann, sowie die Problematik des Schlüsselaustauschs.

4.2. Caesar-Verfahren

Der Anfang der Stunde zum Caesar-Verfahren gleicht dem Anfang der vorangegangenen Stunde. Die Schüler kommen erneut in den Sitzkreis und die neue mit dem Caesar-Verfahren verschlüsselte Nachricht liegt wieder in der Schatzkiste. Was ich mir dabei denke ist, dass die Schüler zunächst erkennen sollen, dass wir

uns weiterhin mit Geheimnissen und Geheimschriften auseinandersetzen, dass sie aber diesmal plötzlich eine Botschaft vorfinden, die auf einem normalen Papier geschrieben steht und die sich nun entsprechend nicht mehr um eine Holzrolle wickeln lässt. Außerdem erhoffe ich mir, dass die Schüler in der Erinnerung an den interessanten Inhalt des Vortages sofort den Inhalt der Truhe sehen möchten, sodass sie sofort motiviert sind ein weiteres Rätsel zu lösen. Um dem historischen Anteil diesmal deutlicher Rechnung zu tragen, habe ich versucht die Nachricht selbst in Form einer Schriftrolle zu gestalten, die dann in der Kiste liegt. Darüber hinaus habe ich den Text aber auch noch einmal für alle Schüler kopiert, sodass sich an der Lösung diesmal auch wirklich jeder beteiligen kann. Bevor die Schüler für die Arbeitsphase an ihre Plätze zurückgehen, betrachten wir das Verfahren genauer. Dabei sollen die unterschiedlichen Möglichkeiten der Verschiebung benannt werden, bis wir schließlich zur Caesar-Scheibe gelangen die uns die Möglichkeit gibt diese Verschiebungen relativ leicht und schnell durchzuführen.

In der Arbeitsphase erhalten die Schüler Materialien um sich eigene Caesar-Scheiben herzustellen. Von den beiden Scheiben ist jedoch nur eine bedruckt, sodass es an den Schülern selbst ist zu entscheiden, wie sie ihre Scheibe beschriften. Ich möchte dabei keine Vorgaben machen und hoffe, dass einige Schüler bemerken werden, dass es keine Rolle spielt in welcher Reihenfolge man die Buchstaben aufschreibt, solange man jeden Buchstaben nur genau einmal verwendet. Eine solche Permutation unseres Alphabets würde einer Brute Force Methode deutlich stärker trotzen. Mit den Scheiben können sich die Schüler gegenseitig Nachrichten schreiben. Dabei sollten sie bemerken, sofern die Schüler unterschiedliche Scheiben basteln, dass man diese nur wieder entschlüsseln kann, wenn man auch wirklich die gleiche Scheibe und die gleiche Einstellung verwendet. Aus den Erkenntnissen einzelner Schüler heraus, ist es dann an allen diese These auszuprobieren. Daraus ergibt sich schließlich auch für das Caesar-Verfahren das Problem des Schlüsselübertrags.

Das Hauptziel der Stunde ist, das Caesar-Verfahren kennen und anwenden zu lernen. Die Feinziele ergeben sich hier aus dem direkten Vergleich zwischen Caesar-Verfahren und der Skytale. Die Schüler erkennen, dass es neben dem Verschieben von Buchstaben (Transposition) auch die Möglichkeit der Ersetzung (Substitution) gibt. Neben den Unterschieden zwischen den beiden Verfahren, gibt es aber auch eine wichtige Gemeinsamkeit, das, nach wie vor bestehende, Problem den Schlüssel

mit zu übermitteln. Diese Erkenntnis zieht sich wie ein roter Faden durch die Stunden zu den symmetrischen Verfahren bis hin zur Stunde, die der Schlüsselverteilung gewidmet ist.

4.3. Vigenère-Verfahren

Der Einstieg zu dieser Stunde verläuft nun anders als die beiden vorangegangenen. Er beginnt noch einmal mit dem Caesar-Verfahren. Ich verteile einen, mit dem Caesar-Verfahren, verschlüsselten Text und bitte die Schüler diesen ohne Wissen über die zugehörige Buchstabenverschiebung zu entschlüsseln. Nachdem sie dann hoffentlich eine kurze Zeit ratlos grübeln, wie man dies anstellen könnte, stelle ich ihnen das Problem der Buchstabenhäufigkeit vor. Der Text wurde von mir so ausgewählt, dass die Schüler ihn anschließend unter Verwendung der Häufigkeitsanalyse entschlüsseln können. Von diesem Problem möchte ich auf das Vigenère-Verfahren kommen, welches einer Häufigkeitsanalyse stand hält. Nach der Vermittlung der Funktionsweise dieses Verfahrens, sollen die Schüler dieses in Partnerarbeit anwenden und auch hier schließlich wieder das Schlüsselproblem erkennen.
Das Hauptziel der Stunde ist das Kennenlernen und Anwenden können der Vigenère-Verschlüsselung. Darüber hinaus lernen die Schülerinnen und Schüler eine große Schwachstelle des Caesar-Verfahrens, sowie das damit verbundene kryptoanalytische Verfahren der Häufigkeitsanalyse kennen. Sie erkennen damit die Überlegenheit des Vigenère-Verfahrens gegenüber der Caesar-Methode, sowie auch bei diesem Verfahren die Problematik des Schlüsselübertrags. Da ich denke, dass das Vigenère-Verfahren ohnehin kompliziert genug ist, verzichte ich auf das Problem des Ermittelns der durchschnittlichen Schlüssellänge.

4.4. Fleissner-Schablone

In dieser Stunde stelle ich die Schüler auch wieder vor ein Problem, allerdings verzichte ich dabei auf die Schatzkiste. Ich lege eine verschlüsselte Nachricht auf den Overheadprojektor. Diese Vorgehensweise bietet sich für die Stunde zur Fleissner-Verschlüsselung deswegen an, weil jeder Schüler das Verfahren an der Wand nachvollziehen kann und man somit nicht für jeden Schüler einzeln eine

Schablone herstellen muss. Das Besondere an der Nachricht, die an der Wand erscheint ist, dass sie in ein quadratisches Raster aus 16 Feldern geschrieben ist (und selbstverständlich keinen Sinn ergibt, wie die Texte in den vorangegangenen Stunden auch). Die Schüler sollen zunächst selbst überlegen, was es mit der Nachricht in dieser merkwürdigen Form auf sich hat. Anschließend zeige ich den Schülern die Schablone und rufe Schülerinnen und Schüler mit Ideen zur Entschlüsselung nach vorne, damit sie ihre Vermutung überprüfen können. Im Anschluss daran sollen die Schülerinnen und Schüler sich eigene Schablonen bauen. Im Gegensatz zu den sonst üblichen nummerierten Schablonenvorlagen, bekommen die Kinder von mir nicht nummerierte Vorlagen. Ich erhoffe mir davon, dass einige Schüler die Vorlagen falsch ausstanzen und im Ergebnis feststellen, dass durch die Drehung nur bestimmte Felder ausgestanzt werden dürfen. Dies möchte ich als Anknüpfpunkt zu einer Diskussion zwischen den Schülern über die Symmetrie der Schablone und die damit verbundene Vorgabe des Ausstanzens nutzen. Anschließend verschlüsseln die Schüler wiederum Texte in Partnerarbeit, wobei sie wieder feststellen sollen, dass man einen geheimen Text nur mit der Schablone entschlüsseln kann, mit der er auch verschlüsselt wurde.
Hauptziel der Stunde ist entsprechend, das Verfahren mit der Fleissner-Schablone, insbesondere wieder das Kennenlernen und die Anwendung. Feinziele sind darüber hinaus die Erkenntnis der Gemeinsamkeit dieses Verfahrens mit der Skytale (Transposition), sowie das Wissen, wie man sich eine eigene Schablone herstellt, bezogen auf die Technik und die Felder, die zu wählen sind und schließlich auch wieder die Kenntnis des Problems der Schlüsselübergabe.

4.5. Schlüsselübertrag

Für den Einstieg zu dieser Stunde habe ich eine Geschichte gewählt. Ich glaube, dass ich die Problematik mit Figuren, welche die Schüler kennen, sehr gut auf den Punkt bringen kann und die Schüler, nachdem ich sie bei jedem einzelnen Verfahren in den vorangegangenen Stunden für dieses Problem sensibilisiert habe, nun endgültig darauf stoßen kann. Nach einer Rücksprache mit Frau Blume wusste ich, dass die Schüler gerne die drei Fragezeichen lesen, also konzipierte ich eine kleine Geschichte, in der diese drei Figuren genau vor dem Problem mit dem Schlüsselübertrag stehen und dieses nicht lösen können. Am Ende steht

entsprechend die Frage, ob die Schüler ihnen helfen können. Zur Lösung dieses Problems dienen Einwegfunktionen der Mathematik. Da die Schüler solche Funktionen aber noch nicht kennen, versuche ich ihnen diesen Weg analog über Farben zu ermöglichen. Zunächst zeige ich zwei Farben und frage die Schüler, ob sie diese zusammenmischen können. Das eigentliche Problem stellt sich erst hinterher, wenn ich den Schülern den Auftrag gebe eine Mischfarbe in ihre ursprünglichen Farbbestandteile zu zerlegen. Wenn die Schüler verstanden haben, dass es Wege gibt, die nur in einer Richtung zu beschreiten sind, dann machen wir uns gemeinsam Schritt für Schritt an die Aufgabe in Partnerarbeit jeweils eine gemeinsame Farbe zu mischen, ohne uns über die endgültige Farbe abzusprechen. Dies funktioniert, indem sich beide Schüler auf eine bestimmte Farbe und eine Menge einigen, die sie dann beide nehmen. In diese Grundfarbe mischt jeder der beiden nun eine Farbe seiner Wahl. Die Menge darf er ebenfalls bestimmen. Anschließend werden die Mischfarben getauscht und jeder der beiden mischt erneut die Farbe seiner Wahl in seiner Menge in den Becher des Partners. Die entstandene Farbe besteht in der Regel aus drei Teilen zu gleichen Mengen, die Grundfarbe, die Farbe des einen Partners und die des Anderen. Zu diesem Zweck stelle ich den Schülern Farben aus dem Baumarkt zur Verfügung. Zum Mischen erhalten sie Plastikbecher. Dem Abmessen der Farben dienen Einwegspritzen.
Das Hauptziel der Stunde ist eine Lösung für das klassische Problem symmetrischer Verschlüsselungsmethoden zu kennen. Feinziele sind dabei die Erkenntnis der Wichtigkeit des Schlüssels, sowie der Problematik seiner Übergabe. Außerdem lernen sie das Prinzip der Einwegfunktion kennen.

4.6. Steganografische Methoden

Diese Stunde bildet das furiose Finale meiner Einheit und dieses beginnt mit einem Effekt, der schon beinahe an einen Zaubertrick erinnert. Ich beschreibe ein Blatt Papier mit Tinte, die empfindlich auf ultraviolettes Licht reagiert, anders ausgedrückt: Bei normalem Licht ist die Tinte unsichtbar, leuchtet man mit UV-Licht darauf, wird die Schrift sichtbar. Ein ähnlicher Effekt folgt sofort, wenn Schrift mit dem Feuer einer Kerze sichtbar gemacht wird. Diese Effekte dienen als Einstieg, weil sie sehr leicht vor der Klasse durchzuführen sind und, wenn ich den Schülern erzähle, dass sie selbst anschließend mit unsichtbarer Tinte arbeiten sollen, erhoffe ich mir eine

unglaubliche Motivation. Tatsächlich möchte ich aber im nächsten Schritt zuerst einmal die Gemeinsamkeiten und Unterschiede zwischen den Verfahren der ersten Stunden und diesem von den Schülern wissen, da ich finde, dass die grundsätzliche Unterscheidung in Kryptographie und Steganografie auch bereits in der Grundschule vorgenommen werden sollte. Ob man die Fachbegriffe gebraucht, oder einfach zwischen „Verschlüsseln“ und „Verstecken“ unterscheidet ist jedem selbst überlassen, ich habe mich für das zweite Vorgehen entschieden, da ich die Schüler während der ganzen Einheit nicht mit zu vielen Fachbegriffen verwirren wollte. Anschließend verteile ich Postkarten mit belanglosen Urlaubsgrüßen. Der aufmerksame Leser bemerkt allerdings relativ schnell, dass einige Buchstaben auf unterschiedliche Art und Weise markiert sind. Liest man nur diese Postkarten, ergibt sich eine andere, geheime, Botschaft. Außerdem lernen die Kinder klassische Verfahren wie den Mikropunkt, das Tätowieren von Sklaven oder Schmuggeln von Nachrichten in Tierkadavern kennen. Dann basteln wir mit Strohhalmen, Watte, Schaschlikspießen und Zitronensaft Geheimstifte. Die Watte wird zerpflückt und mit Hilfe des Schaschlikspießes in den Strohhalm gedrückt. Wenn der Strohhalm etwa zu drei Vierteln mit Watte gefüllt ist, kommt ein kleines festes Wattekügelchen an die Unterseite des Strohhalms. Nun kann man den Strohhalm mit Zitronensaft aufziehen, sodass er diesen, ähnlich einer Kugelschreibermine speichert und anschließend damit schreiben. Der getrocknete Zitronensaft wird über der Kerzenflamme wieder sichtbar.

Das Hauptziel dieser Stunde ist eigentlich das Kennenlernen der Steganografie. Dabei sollen die Schüler den Unterschied zwischen Kryptographie und Steganografie verstehen, sie erkennen, dass man Nachrichten nicht nur verschlüsseln, sondern auch verstecken kann und lernen klassische Verfahren der Steganografie kennen. Den Höhepunkt der Stunde bietet die Anfertigung des eigenen Schreibers, der mit Zitronensaft gefüllt wird und anschließend zum Schreiben geheimer Botschaften genutzt werden kann.

5. Reflexion der einzelnen Stunden

Im Folgenden möchte ich nachträglich den Verlauf jeder einzelnen Stunde skizzieren und reflektieren was gut verlief, was weniger gut verlief und worauf ich beim nächsten Mal besonders achten bzw. was ich beim nächsten Mal anders machen würde.

5.1. Skytale von Sparta

Der Einstieg der Stunde hat den gewünschten Effekt gebracht. Die Neugier der Schüler war schon bei der ersten Sichtung der Schatztruhe geweckt. Als problematisch erwies sich hingegen das Öffnen der Kiste und die verschlüsselte Nachricht selbst, da den Schülerinnen und Schülern sofort klar war, dass man den Streifen um das Holzstück wickeln muss, aber jeder dies ausprobieren wollte. Ich habe daraufhin mehrere weitere Nachrichten und Holzstücke (in unterschiedlicher Dicke) in der Runde verteilt. Die folgende Arbeitsphase und der Austausch unter den Schülern war sehr fruchtbar, so fanden wir gemeinsam heraus, worauf es eigentlich bei der Skytale ankommt, nämlich auf den Umfang des Holzstückes. Darüber hinaus erkannten wir aber auch Probleme im Umgang mit dem Verfahren als einige Schüler das Band von rechts nach links aufwickelten oder zwar links anfingen aber in der falschen Richtung wickelten. Ich widmete der Diskussion der Probleme dann die Zeit, die ich eigentlich eingeplant hatte, um den Bezug zu den Geheimnissen der Schüler herzustellen, denn es schien mir, dass ohnehin jedem Schüler klar war, dass er Geheimnisse besitzt und diese geschützt werden müssen, damit sie eben geheim bleiben. Leider musste auch die Erklärung der Grundbegriffe abgekürzt werden, aber als ich diese anschließend wie selbstverständlich verwendete, hatte keine Schülerin und kein Schüler Verständnisschwierigkeiten. Die Arbeitsphase verlief weitgehend positiv. Es zeigte sich, dass die meisten Schüler keine Probleme mit der Umsetzung des Verfahrens hatten. Sie waren motiviert und engagiert. Lediglich zwei Schüler schrieben Silben anstelle einzelner Buchstaben auf die Streifen, sodass die Sicherheit stark abnahm. Nach einer Erklärung sahen sie das jedoch ein. Ein großer Fehler meinerseits bestand darin, dass ich zu wenige Streifen vorbereitet hatte. Zu meinem Glück waren es nur zwei Schüler gewesen, die bei der Anwendung des Verfahrens Probleme hatten, allerdings wollte fast jeder Schüler eine zweite oder

dritte Nachricht schreiben für die ich kein Material mehr hatte. Die Besprechung des Problems mit der Übertragung des Schlüssels entfiel aus Zeitgründen. Abschließend denke ich, dass es eventuell sinnvoll gewesen wäre den Einstieg in die Einheit in einer Doppelstunde vorzunehmen. Im heutigen Computerzeitalter ist nämlich nicht jedem Schüler sofort klar, wieso man Briefe, die verschickt wurden verschlüsseln musste. Auf diesen historischen Aspekt des Überbringens der Nachricht selbst könnte man dann einen viel stärkeren Bezug nehmen. Außerdem führen die Probleme bei der Entschlüsselung der ersten Nachricht nicht zum Wegfall des Alltagsbezuges, sowie dem Problem des Schlüsselübertrags und zur Einschränkung der Klärung von Grundbegriffen. Zu einem Leerlauf wird es in einer solchen Doppelstunde nie kommen, wenn man den Schülern nur genügend Stoffbänder zur Verfügung stellt, denn die möchten am liebsten jedem ihrer Freunde oder Freundinnen eine Nachricht schreiben.

5.2. Caesar-Verfahren

Die Stunde zum Caesar-Verfahren begann etwas anders als der Plan dies vorsah. Da wir in der vorangegangenen Stunde die Probleme der Skytale nicht durchgenommen hatten, rekapitulierten wir zu Beginn dieser Stunde gemeinsam noch einmal was wir am Vortag besprochen hatten und überlegten gemeinsam nach Problemen. Tatsächlich fiel es den Schülern nicht schwer die Probleme der Skytale in Worte zu fassen: „falsch herum wickeln“, „auf der falschen Seite anfangen“, „mehrere Buchstaben oder Silben auf einen Streifenabschnitt schreiben“, sowie „der unterschiedliche Umfang des Holzes“ und damit verbunden das Problem „das Holz mit der Nachricht mitschicken zu müssen“. Ein wichtiges Problem ergab sich aus der Überlegung das Holz getrennt von der Nachricht zu übermitteln. Ein Schüler sagte: „Wenn man aber nur die Nachricht ohne das Holz hat, dann kann man schon an dem Streifen erkennen, dass das um ein Holz gewickelt werden muss und dann kann man das ja einfach so lange ausprobieren, bis es passt.“ Ohne es zu wissen, hat dieser Junge eine wichtige kryptoanalytische Methode auf die Nachricht angewendet, nämlich die des Brute Force. Genau diese Problematik war es, die alle Schüler verstanden und die sie in Erstaunen versetzte, als die nächste Botschaft auf einem normalen Papier stand, das man nicht um ein Holz wickeln konnte. Doch noch bevor ich die Kiste hervorholen konnte, in der die neue Nachricht, mittels der Caesar-

Methode verschlüsselt, lag, meldete sich ein Schüler und sagte: „wir können ja auch mal das von dem Caesar machen. Der hat nämlich zwei so runde Steine genommen und das Alphabet da rein geschrieben und dann konnte der die so verdrehen, dass ein Buchstabe ein Anderer war und dann hat er den Anderen aufgeschrieben.“ Selbst wer die Caesar-Methode nicht kennt, kann das Verfahren in diesen kindlichen Worten verstehen. Ich habe versucht dem Schüler zu zeigen, wie toll ich es finde, dass er sich mit so etwas auskennt und ihn darin bestärkt weiter so neugierig zu sein. Schließlich habe ich ihn zum Experten für die anstehende Stunde benannt und er konnte an der ersten Nachricht noch einmal für alle genau erklären, wie ich diese vorbereitet hatte und wie man dies nun mit Hilfe der Scheibe, die ich ihm dann auch eingestellt gegeben habe, entschlüsseln kann. Besser als dieser Schüler es seinen Mitschülerinnen und Mitschülern erklärte, hätte ich das wohl auch nicht hinbekommen. Jeder hatte das Verfahren verstanden. Leider zeigte sich hier das wahrscheinlich größte Problem der Stunde: Der Text, den ich den Schülern verschlüsselt vorgelegt hatte (siehe Anhang) erwies sich nicht nur als ein wenig zu lang, sondern als viel zu lang. Zwar konnten wir anschließend zum Basteln der Scheiben übergehen, allerdings hatten die Schüler dann nur noch wenig Zeit für die Anwendung des Verfahrens. Leider war kein Schüler dabei, der beim Basteln der Scheiben auf die Idee kam die kleinere Scheibe durcheinander zu beschriften. Meine Bemühungen sie auf diese Idee zu bringen waren deplaziert, da die Schülerinnen und Schüler nicht mir, sondern ihrer Arbeit die Aufmerksamkeit widmeten, sodass ich schlichtweg nicht beachtet wurde. Das Problem, dass auch hier die Scheiben, bzw. da ja nun am Ende alle Schüler die gleiche Scheibe hatten, sie hatten sie ja gerade gleichmäßig beschriftet, die Scheibenstellung, mit übertragen werden musste war allen Schülern klar. Einige kamen sogar auf die Idee diese Stellung in Form der Ziffer um die Verschoben wurde an den Anfang der Nachricht zu stellen. Sie merkten allerdings relativ schnell, dass wenn das Verfahren bekannt ist, dies dazu führt, dass jeder mit Hilfe dieser Ziffer den Text entschlüsseln kann.

5.3. Vigenère-Verfahren

Betrachtet man das Hauptziel der Stunde (Kennenlernen und Anwendung des Vigenère-Verfahrens) könnte man vielleicht behaupten, die Stunde sei ein Erfolg gewesen. Dies wäre aber im besten Falle die halbe Wahrheit. Der Grund, weshalb diese Stunde schief lief, liegt allerdings bei mir, ich habe sie schlichtweg in den Sand gesetzt. Während der Aufbau meiner Meinung nach stimmig war, bzw. immer noch ist, habe ich die Schüler in den einzelnen Bereichen total überfordert. Es war eine sehr gute Idee mit der Häufigkeitsanalyse zu beginnen. Nachdem die Schüler den Text geknackt hatten, wussten sie, dass diese kryptoanalytische Methode funktioniert und ein stärkeres Verfahren her muss. Leider war zu diesem Zeitpunkt aber auch schon gut die Hälfte der Zeit verstrichen, denn es war für die Schüler zu kompliziert gleich mehrere verschiedene Buchstaben zu ermitteln von denen sich einige nicht in der Häufigkeit unterschieden. Die Idee ist gut, allerdings wäre es sinnvoll gewesen die Häufigkeitsanalyse auf die zwei bis drei häufigsten Buchstaben in unserem Alphabet zu beschränken, sodass die Schüler erkennen, dass das Caesar-Verfahren keine ausreichende Sicherheit bietet, dies aber in einem zeitlich vernünftigen Rahmen schaffen. Dies ist aber leider nicht der einzige Grund, weshalb die Stunde aus den Angeln gehoben wurde. Nachdem die Häufigkeitsanalyse erfolgreich beendet war, stellte ich das Vigenère-Verfahren vor. In der Erwartung ein sicheres Verfahren kennengelernt zu haben, stürzten sich die Schülerinnen und Schüler auf die Aufgabe die ich ihnen gegeben hatte und diese Aufgabe war aufgrund des Stundenaufbaus praktisch nicht lösbar. Ich hatte den Schülern nämlich erklärt, wie man mit Hilfe der Vigenère-Tafel Texte verschlüsselt, da ich es bei der Vorbereitung aber für „spannender“ hielt die Schüler einen Text entschlüsseln zu lassen, bekamen sie nun einen verschlüsselten Text, den sie, nach der Methode, wie ich es ihnen erklärt hatte, ein weiteres Mal überschlüsselten und somit kein sinnvolles Ergebnis erhielten. Es war für die Schüler, die niemals zuvor eine Vigenère-Verschlüsselung durchgeführt hatten logischerweise nicht nachvollziehbar, wieso ich ihnen erklärt hatte, dass sie den Klartextbuchstaben in der obersten Zeile suchen müssen und den Schlüsselbuchstaben in der ersten Spalte um am Kreuzungspunkt den Geheimtextbuchstaben zu finden und genau dieses Verfahren jetzt falsch sein sollte, weil sie in der Zeile, die der Schlüsselbuchstabe markierte bereits den verschlüsselten Buchstaben suchen mussten um auf den Klartextbuchstaben zurück

zu kommen. Dieser Rückweg erschließt sich ja gerade erst dadurch, dass man das Verfahren einmal auf dem Hinweg ausprobiert hat, oder wenn man über ein starkes Abstraktionsvermögen verfügt. Nach weiteren Erklärungsversuchen gelang es schließlich den stärksten Schülern den Text zu entschlüsseln. Die Übrigen schrieben das Ergebnis ab, oder gaben einfach auf. Hätte ich die Schüler einen Text verschlüsseln lassen, hätten sicherlich alle ein zufrieden stellendes Ergebnis erzielt und viele die Erkenntnis gehabt, wieso der Rückweg anders aussehen muss, so allerdings, verschloss sich diese Erkenntnis fast allen. Allein die Tatsache, dass trotz meiner absolut fehlgeleiteten Vorbereitung dennoch zwei Schüler (wenngleich es die beiden Klassenstärksten waren) am Ende verstanden, wieso der Weg vom verschlüsselten Text zum Klartext ein anderer ist und ein Ergebnis erzielten, zeigt mir aber, dass auch Grundschüler der vierten Klasse grundsätzlich in der Lage sind dieses Verfahren zu verstehen.

5.4. Fleissner-Schablone

Diese Stunde verlief zum Glück besser als die Vorangegangene und trotz der desaströsen Stunde zuvor, waren die Schüler nach wie vor neugierig auf mehr. Vielleicht ist dies auch der Tatsache zu verdanken, dass zwischen den beiden Stunden eine Woche Faschingsferien ins Land gezogen war, sodass sie ein wenig Abstand gewinnen konnten. Nach dem hoffnungslosen Umgang mit dem Vigenère-Verfahren kam den Schülern diese Methode jedenfalls sehr gelegen, zumal ich es stark handlungsorientiert angelegt hatte, da die Schüler sich ihre Schablonen ja ohne Vorgabe selbst herstellen durften. Doch ich will am Anfang beginnen. Der Einstieg war ziemlich schnörkellos, aber dem Thema angemessen. Die Schüler erkannten die merkwürdige Anordnung der Buchstaben, konnten damit aber zunächst nichts anfangen. Als ich die Schablone zeigte, war eigentlich allen klar, was damit anzufangen war und so verwundert es nicht, dass fast alle Finger nach oben gingen, weil jeder den Text entschlüsseln wollte. Interessanterweise gelang es dem ersten Schüler, den ich nach vorne holte sämtliche Fragen aufzuwerfen, die mit der Fleissner-Schablone in Zusammenhang stehen. Zunächst legte er die Schablone mit der Oberseite nach unten auf die Buchstaben, sodass sich kein sinnvoller Text ergab. Dann hatte er zwar die richtige Seite oben, begann aber in der falschen Ecke und schließlich drehte er die Schablone auch noch gegen den Uhrzeigersinn. Damit

hatten eigentlich alle Schüler die Probleme erkannt, wir haben sie noch einmal gesammelt, bzw. benannt und uns schließlich auf einige Standards im Umgang mit der Schablone geeinigt, die da wären „Bedruckte Seite nach oben“, „rechte obere Ecke als solche markieren“ und „im Uhrzeigersinn drehen“. Im Anschluss daran durften die Schüler sich ihre Schablonen herstellen. Tatsächlich passiert es einigen, dass sie manche Felder doppelt oder gar dreifach ausschlugen, andere wurden gleich ganz ausgelassen. Dies erkannten die Schüler aber bei dem Erstellen des Textes selbst sofort. Zum Glück hatte ich diesmal nicht den Fehler gemacht zu wenig Material zur Verfügung zu stellen, sodass genügend Vordrucke für alle vorhanden waren. Einige Schüler ließen sich nicht einmal in die große Pause schicken, als es zum Ende der Stunde geläutet hatte.

5.5. Schlüsselübertrag

Die Stunde zur Schlüsselverteilung stand unter keinem guten Stern. Es war die Stunde mit der ich am meisten haderte, von der ich am wenigsten überzeugt war und wenn man von einer Sache nicht überzeugt ist, sollte man sie eigentlich auch nicht unterrichten oder es wird sehr schwer werden. Die Zweifel kamen von Seiten der Klassenlehrerin. Frau Blume meinte, den Schülern würde das Abstraktionsvermögen fehlen, um zu erkennen, dass es sich bei der Farbenmischerei nur um eine Analogie handele und wenn diese Erkenntnis fehle, dann wäre es den Schülern nicht ersichtlich, wieso diese Farben jetzt ein Schlüssel sein sollen, wo sie doch vorher mit Skytalen, Caesar-Scheiben-Stellungen, Schlüsselwörtern und Schablonen gearbeitet hatten. Wenn aber diese Einsicht fehlt, dann fehlt auch der gesamte Zusammenhang zwischen dieser Stunde und der gesamten Einheit. Ich habe mich dennoch entschieden sie durchzuführen, weil ich wissen wollte, wie weit das Verständnis der Schüler ausreicht. Tatsächlich war es für die Schüler kein Problem das Prinzip der Einwegfunktion zu verstehen. Das sie selbst zwei zusammen gemischte Farben nicht wieder „entmischen“ können, war allen klar. Tatsächlich führte das anschließende Experiment zu dem gewünschten Ergebnis. Fast alle Partner hatten am Ende des Mischens die gleiche Farbe erhalten. Dieses Resultat führte zu Verwunderung bei den Schülern. Viele kamen mit ihren Farben auf mich zu und sagten „Schau mal, wir haben ja die gleiche Farbe“. Das Experiment hatte also geklappt und die Verwunderung war groß, denn die Schüler hatten sich ja, bis auf die Wahl der

Grundfarbe, nicht abgesprochen. Dennoch muss ich nachträglich zugeben, dass sich die Befürchtungen von Frau Blume bestätigten. Zwar hatten die Schüler den gewünschten Effekt erreicht, sie wussten allerdings nichts damit anzufangen. Da ich ihnen nun aber nicht erklären wollte, dass ihre Mischung nur ein Stellvertreter für eine mathematische Funktion sei, die sie nicht verstehen konnten, bot ich ihnen an die Farbe zu benennen und das Wort, also den Farbennamen als Schlüssel zu verwenden. Dies trug allerdings dem Verfahren nicht Rechnung, denn es führte dazu, dass die jeweiligen Partner sich wieder auf einen Namen einigen mussten. Außerdem nutzte nur ein Paar diese Möglichkeit aus um wirklich eine Nachricht zu verschlüsseln.

Diese Stunde würde ich so in einer vierten Klasse sicherlich nicht wieder halten. An dieser Stelle möchte ich Herrn Bohrmann zitieren, der einmal in einer Vorlesung sagte: „Eine Stunde die nur irgendeinen Effekt bietet ohne Erklärungsgehalt oder Bedeutung gehört nicht in die Schule, sondern allerhöchstens auf den Kindergeburtstag.“ Ich bin nun ebenfalls davon überzeugt, dass den Schülern der vierten Klasse das Abstraktionsvermögen fehlt um sinnvolle Erkenntnisse aus diesem Vorgang zu gewinnen. Das Problem des Schlüsselübertrags zu benennen empfinde ich allerdings nicht nur als sinnvoll, sondern aufgrund der Wichtigkeit und der zentralen Stellung dieses Problems innerhalb der Kryptographie auch für geboten. Gegebenenfalls könnte man dies aber besser mit einem Ausflug zu den heute gebräuchlichen asymmetrischen Verfahren verbinden. Denn die grundlegende Funktion solcher asymmetrischer Verfahren erschließt sich auch anhand eines Vorhängeschlosses (jeder kann es einschnappen lassen, doch nur der mit dem privaten Schlüssel kann es wieder öffnen) ohne irgendein spezielles Verfahren zu kennen. Andererseits stellt sich die Frage, ob unsere Grundschüler überhaupt eine Lösung für dieses Problem kennen müssen, denn immerhin sind ihre vertraulichen Nachrichten meist nicht von Geheimdiensten bedroht. Die Erwähnung des Problems lässt sie vielleicht sorgsamer mit dem Schlüssel umgehen, doch diesem Problem eine ganze Schulstunde in einer Grundschule zu widmen halte ich heute eigentlich für unangebracht.

5.6. Steganografische Methoden

Diese Stunde verlief sehr ähnlich zu meiner Planung. Die Schüler waren von dem Geheimschreiber sofort begeistert und auch das Sichtbarwerden der Nachricht die ich mit Zitronensaft vorbereitet hatte erzielte seine Wirkung. Der Unterschied zwischen den kryptographischen und den steganografischen Verfahren war allen sofort klar. Wie gebannt lauschten sie meinen Ausführungen zu den klassischen Verfahren, insbesondere die Sklaventätowierung riss sie mit und es kamen immer wieder nachfragen der Art „Wie haben die das denn damals gemacht?“. Das basteln des eigenen Geheimschreibers bereitete allen große Freude. Gefährlich wurde es beim Sichtbarmachen dessen, was sie mit ihrem Stift geschrieben hatten. Leider müssen die mit Zitronensaft geschriebenen Worte erst trocknen, bevor man sie über dem Feuer sichtbar machen kann. Das war im Rahmen einer einzelnen Stunde kaum möglich. Frau Blume empfahl anschließend die Stunde doppelstündig anzulegen und am Anfang die Stifte zu bauen und die Nachrichten schreiben zu lassen, dann den Exkurs über die klassischen Verfahren und insbesondere die Postkarten länger zu behandeln, da die Schüler großes Interesse an den Postkarten hegten. Nachdem sie einmal erkannt hatten, dass Buchstaben markiert worden waren, wollte jeder Schüler, jede Postkarte einmal in der Hand gehalten und entziffert haben, doch dafür reichte die Zeit leider nicht. Da der Zeitdruck nun aber dazu führte, dass viele Nachrichten am Ende nicht mehr trockneten und dadurch unsichtbar blieben, gingen die Schülerinnen und Schüler immer knapper über die Kerzenflamme und einige Blätter fingen Feuer. Da ich dieses Verfahren im Vorfeld ausprobiert hatte und mir das gleiche passiert war, war ich darauf vorbereitet gewesen. Ich hatte extra Seiten mit Rändern bedruckt in denen die Schüler schreiben und sie anschließend außen festhalten konnten ohne sich die Finger zu verbrennen. Außerdem hatte Frau Blume zu dem Zeitpunkt, da ich diese Stunde durchführte eine Praktikantin, sodass drei Erwachsene im Raum waren. Ich hatte extra nur drei Kerzen mitgebracht und jeder Kerze einen Wassereimer und einen Erwachsenen zur Seite gestellt. Dennoch gerieten einige Schüler in Panik als die Blätter in Flammen aufgingen und warfen diese wild weg, anstatt sie in den Wassereimer zu werfen. Ich kann an dieser Stelle nur dringend dazu raten solche Experimente niemals alleine vor einer Klasse durchzuführen. Trotz einzelner Panikreaktionen waren die Schüler begeistert. An eine Pause war auch diesmal nicht zu denken. Einige Zeit nach der Einheit bekam

ich einen Brief von der Klasse. Jeder Schüler hatte einen eigenen Brief verfasst, in dem er mir mitteilte, was ihm an der Einheit am besten gefallen hat und diesen Brief in den Umschlag gesteckt. Ein großer Anteil der Briefe zeigte sehr deutlich, dass die unsichtbare Tinte und das wieder Sichtbarmachen mit der Kerze der Favorit unter den Schülern war.

6. Reflexion der gesamten Einheit

Das Ziel der Einheit war den Schülern zu zeigen, dass jeder Mensch Geheimnisse hat, dass wir diese auch brauchen und dass es Möglichkeiten gibt unsere Geheimnisse auch wirklich geheim zu halten, nämlich mit Hilfe der Kryptologie. Ich denke, dass dieses Ziel auch im Großen und Ganzen erfüllt wurde. Sicherlich hat nicht jeder Schüler jedes Verfahren verstanden und einiges würde ich sicherlich anders gestalten, wenn ich noch einmal eine Einheit zu Geheimschriften machen würde, doch zunächst möchte ich sagen, dass ich die Einheit selbst als sehr gewinnbringend für alle beteiligten einschätze und eine solche Einheit jederzeit wieder durchführen und auch allen anderen dazu raten würde. Bestärkt wurde ich in dieser Meinung durch Schülerrezensionen. Das Fazit der Schüler ist sehr positiv ausgefallen, sodass ich schätze, dass sie mir auch den Ratschlag geben würden, Geheimschriften in der Schule zu unterrichten.
Die Skytale und das Caesar-Verfahren gelten heutzutage ja schon fast als die klassischen Verschlüsselungsalgorithmen, die in der Schule vermittelt werden. Das hat auch durchaus seine Gründe, da sie einerseits leicht verständlich sind und andererseits vielfältige Möglichkeiten zu handlungsorientierten Phasen bieten, nämlich gerade nicht nur die Durchführung des Verfahrens selbst, sondern auch die Herstellung einer einfachen Skytale oder Caesar-Scheibe. Die Fleissner-Schablone würde ich in diese Riege mit einordnen, die Herstellung der Schablone gefällt den Schülern sehr, allerdings muss man hier etwas vorsichtig sein, da die Schüler vor lauter Ausschlagen evtl. das Wesentliche, nämlich das Verfahren selbst, vergessen könnten. Außerdem gibt es viele Falltüren, die dazu führen, dass das Verfahren gegebenenfalls schief läuft, z.B. wenn die Schablone falsch herum aufgelegt oder falsch herum gedreht wird, was zu Frustrationen führen kann. Die Skytale weist aber ähnliche Stolpersteine auf (falsches Umwickeln). Die Vigenère-Tafel ist schon etwas komplexer und Frau Blume meinte in einer Reflexion zu mir, dass sie diese Stunde

vielleicht weglassen würde, ich sehe das etwas anders, da ich denke, dass es die Schüler über den Zugang der Häufigkeitsanalyse von Buchstaben geradezu nach einem Verfahren dürstet, dass einer solchen Analyse stand hält. Ich habe mir leider selbst ein Bein gestellt, indem ich die Stunde zum Vigenère-Verfahren falsch herum aufgezogen habe (siehe Punkt 4.3.). Ich bin allerdings nach wie vor überzeugt, dass eine durchdachtere Herangehensweise den Schülern das Verfahren klarmacht und dass sie im Anschluss daran auf die Umkehrung selbst kommen. Die Stunde zur Schlüsselübergabe war wohl die Schwierigste und ich würde sie auch so nicht mehr halten. Ich wollte diese Stunde durchführen, weil ich testen wollte, wie weit ich gehen kann und wie weit das Verständnis der Viertklässler reicht. Mit dieser Stunde hadere ich auch jetzt noch, nicht etwa, weil ich sie schließlich doch durchgeführt habe, sondern weil ich noch immer nicht weiß, wie ich die Stunde jetzt halten würde. Ich würde sie sicherlich nicht mehr so planen, doch ich finde nach wie vor, dass man die Problematik ansprechen sollte. Diese wurde von den Schülern ja auch sofort verstanden, allerdings fehlt es einfach am Verständnis für das Diffie-Hellman-Verfahren. Wahrscheinlich wäre es hier sinnvoller Viertklässlern die asymmetrische Verschlüsselung mit Hilfe eines Vorhängeschlosses nahe zu bringen. Wenngleich sie kein konkretes Verfahren zur Umsetzung haben, so sind sie doch für das Problem des Schlüsselaustausches sensibilisiert und wissen im Grunde genommen, wie dieses Problem heute gelöst wird. Wenn man damit noch den Anreiz schafft, dass sich einige Schüler selbst weiter mit der Materie beschäftigen und versuchen herauszufinden wie ein Verfahren zum Erzeugen eines Schlüsselpaares funktioniert, dann ist man, glaube ich, auf einem fantastischen Weg. In den oben erwähnten Briefen der Schüler ging sehr deutlich hervor, dass fast die Hälfte der Klasse die Stunde zur Steganografie am besten fand, oder wie sie es ausdrückten „das mit dem Feuer“. Ich finde, dass die Stunde optimal platziert war. Es war noch einmal ein furioses Finale der Einheit und beleuchtete eine andere Seite der Geheimhaltung, nämlich die Steganografie, also nicht das Verschlüsseln, sondern das Verstecken von Nachrichten. Der Steganografie würde ich zukünftig wohl etwas mehr Aufmerksamkeit schenken, da die Postkarten den Rätselgeist weckten, wir allerdings viel zu wenig Zeit dafür hatten. Der Einsatz des Zitronensaftes und des Feuers ist mit Vorsicht zu genießen und bedarf auf jeden Fall der Hilfe mehrerer erwachsener Helfer. Würde man diese Stunde aber streichen, würde man sich ins eigene Fleisch schneiden. Natürlich wüssten die Schüler nicht was sie verpassen, aber man selbst

würde auch nicht die großen Augen und erstaunten Blicke der Schüler sehen, wenn auf einem leeren Blatt plötzlich Buchstaben erscheinen.

7. Fazit

Ich kann nur noch einmal zusammenfassend wiederholen: Die Thematik der Geheimschriften übt auf die Schüler einen so großen Reiz aus, dass die Stunden fast zum Selbstläufer werden. Mein Fazit fällt daher äußerst positiv aus: Ich würde es jederzeit wieder tun, wenngleich ich in einigen Details andere Wege gehen würde, aber es ist ja auch noch kein Meister vom Himmel gefallen, außerdem gehört das immer wieder umgestalten von Stunden und Einheiten ja auch zum Lehrerberuf dazu.
Um die Eindrücke der Schüler zu verdeutlichen, habe ich ihre Briefe eingescannt und im Anhang der Arbeit beigelegt.

Literaturverzeichnis

- Arnold, Patricia: Einsatz digitaler Medien in der Hochschullehre aus lerntheoretischer Sicht.
- Bauer, Friedrich: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie., 2. Auflage, Springer Verlag, Berlin/Heidelberg, 1997.
- Baumgart, Franzjörg (Hrsg.): Entwicklungs- und Lerntheorien. Erläuterungen – Texte – Arbeitsaufgaben., Verlag Julius Klinkhardt, Bad Heilbrunn, 1998.
- Beutelspacher, Albrecht: Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen., 8. Auflage, Vieweg Verlag, Wiesbaden, 2007.
- Bildungsplan 2004 Baden-Württemberg Grundschule, Ministerium für Kultus, Jugend und Sport.
- Bildungsplan 2004 Baden-Württemberg Gymnasium, Ministerium für Kultus, Jugend und Sport.
- Bildungsplan 2004 Baden-Württemberg Hauptschule, Ministerium für Kultus, Jugend und Sport.
- Bildungsplan 2004 Baden-Württemberg Realschule, Ministerium für Kultus, Jugend und Sport.
- Brockhaus – Die Enzyklopädie in vierundzwanzig Bänden, Weltbild Studienausgabe, 20. Auflage, F. A. Brockhaus Verlag, Leipzig, 2001.
- Buth, Manfred: Lerntheorien mit Anwendungen im Mathematikunterricht und im naturwissenschaftlichen Aufgabenfeld., Verlag Franzbecker, Bad Salzdetfurth ü. Hildesheim, 1995.
- Dewey, John: Demokratie und Erziehung, 3. Auflage, Beltz Verlag, Weinheim/Basel, 2000.
- Duden – Deutsches Universalwörterbuch, 6. Auflage, Bibliographisches Institut, Mannheim, 2006.
- Ertel, Wolfgang: Angewandte Kryptographie, Carl Hanser Verlag, München/Wien, 2001.
- Fleissner von Wostrowitz, Eduard: Handbuch der Kryptographie. Anleitung zum Chiffrieren und Dechiffrieren von Geheimschriften., Selbstverlegung des Verfassers, Wien, 1881.

- Kippenhahn, Rudolf: Verschlüsselte Botschaften. Die Geheimschrift des Julius Caesar. Geheimschriften im I. und II. Weltkrieg. Das Codebuch des Papstes. Enigma., 4. Auflage, Nikol Verlag, Hamburg, 2006.
- Kuchenbrod, Stefan: Moderne kryptographische Verfahren im Mathematikunterricht der Sekundarstufe am Beispiel der RSA-Verschlüsselung.
- Pincock, Stephen / Frary, Mark: Geheime Codes. Die berühmtesten Verschlüsselungstechniken und ihre Geschichte., Ehrenwirt in der Verlagsgruppe Lübbe, Bergisch Gladbach, 2007.
- Schmeh, Klaus: Kryptographie. Verfahren, Protokolle, Infrastrukturen., 3. Auflage, dpunkt.Verlag, Heidelberg, 2007.
- Schmeh, Klaus: Versteckte Botschaften. Die faszinierende Geschichte der Steganografie., 1. Auflage, Heise Zeitschriften Verlag, Hannover, 2009.
- Schneier, Bruce: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C., Addison-Wesley Verlag, München, 1996.
- Selter, Christoph / Sundermann, Beate: HFIFJN!., In: Die Grundschulzeitschrift 163, Erhard Friedrich Verlag, Seelze, 2003.
- Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet., 4. Auflage, Deutscher Taschenbuch Verlag, München, 2003.
- The New Encyclopedia Britannica, Volume 3, 15. Auflage, Encyclopedia Britannica Inc., Chicago, 2002.
- Wagenschein, Martin: Verstehen lehren. Genetisch – sokratisch – exemplarisch., 8. Auflage, Beltz Verlag, Weinheim/Basel, 1989.
- Wätjen, Dietmar: Kryptographie. Grundlagen, Algorithmen, Protokolle., Spektrum Akademischer Verlag, Heidelberg/Berlin, 2004.
- Wittenberg, Alexander Israel: Bildung und Mathematik, 2. Auflage, Klett Verlag, Stuttgart, 1990.
- Wittmann, Erich: Grundfragen des Mathematikunterrichts, 6. Auflage, Vieweg Verlag, Braunschweig, 1981.
- Wobst, Reinhard: Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung., 3. Auflage, Addison-Wesley Verlag, München, 2001.
- Wrixon, Fred: Geheimsprachen. Codes, Chiffren und Kryptosysteme. Von den Hieroglyphen zum Digitalzeitalter., Tandem Verlag, München, 2006.

- Ziegenbalg, Jochen / Oliver / Bernd: Algorithmen. Von Hammurapi bis Gödel., 2. Auflage, Wissenschaftlicher Verlag Harri Deutsch, Frankfurt am Main, 2007.
- Ziegenbalg, Jochen: Codierung und Kryptographie, Skript zur Vorlesung „Codierung und Kryptographie“.
- Ziegenbalg, Jochen: Public Key Cryptographie, Notebook zur Vorlesung „Codierung und Kryptographie“.

Internet – Quellenverzeichnis

- http://de.encarta.msn.com
- http://dict.leo.org
- http://erl.orn.mpg.de
- http://homepage.uibk.ac.at
- http://homepages.tscnet.com
- http://lexikon.meyers.de
- http://seegras.discordia.ch
- http://www.bitkom.org
- http://www.bpb.de
- http://www.britannica.com
- http://www.cdc.informatik.tu-darmstadt.de
- http://www.datenschutz-praxis.de
- http://www.heise.de
- http://www.itwissen.info
- http://www.kryptographiespielplatz.de
- http://www.praxis-lexikon.de
- http://www.ulm.ccc.de
- http://www.usncva.org
- http://www.vision-ing21.de
- http://www.wikipedia.de

Abbildungsverzeichnis

Anhang

I. Weiterführender geschichtlicher Einblick

1. Zur vorchristlichen Zeit

1.1. Der Diskos von Phaistos (ca. 17. Jh. v. Chr.)

Aus etwa dem 17. Jh. v. Chr. stammt eine Terracottascheibe, die den Wissenschaftlern bis heute Rätsel aufgibt. Der Diskos von Phaistos wurde 1908 bei Ausgrabungen an einem minoischen Palast auf der Insel Kreta von dem italienischen Archäologen Luigi Pernier gefunden. Die Scheibe besitzt einen Durchmesser von ca. 15 cm und ist beidseitig mit Symbolen bedruckt, die durch Trennlinien in Symbolgruppen geordnet sind. Insgesamt sind es 242 Zeichen in 61 Gruppen zusammengefasst, davon 123 in 31 Gruppen auf der einen und 119 in 30 Gruppen auf der anderen Seite. Allerdings enthält der Diskos nur 45 unterschiedliche Symbole, von denen viele sehr leicht zu erkennen sind (alltägliche Symbole wie Menschen, Tiere, Objekte, usw.). Wissenschaftler fanden heraus, dass die Symbole auf der Scheibe nicht geritzt oder gemeißelt wurden, sondern mit Prägestempeln eingehauen wurden, was sie vermuten lässt, dass es sich aufgrund der Komplexität solcher Siegel um Zeichen handelt, die sehr oft eingesetzt wurden. Gleichzeitig wurde aber nie ein anderes Artefakt gefunden, welches die gleichen Zeichen verwendet und genau da liegt das Problem, aufgrund fehlender Ressourcen lässt sich die Verwendung der Zeichen nicht eindeutig bestimmen. Die Wissenschaft ist sich über die Bedeutung der Scheibe uneinig, einige Wissenschaftler glauben es könne sich um eine Art Kalender handeln, Andere tippen auf den Aufschrieb eines Gebetes, eine Frage an ein Orakel oder einen Aufruf zum Kampf. Wieder Andere glauben, dass es sich um ein Spielbrett oder ein geometrisches Theorem handelt. Viele Experten glauben allerdings, dass die Mythen um den Diskos von Phaistos

nicht zu klären sind, da er zu wenig Schriftzeichen enthalte und weitere Schriftstücke, aus denen man Schlussfolgerungen auf den Einsatz ziehen könnte, fehlen.[203]

1.2 Linear A und Linear B (ca. 2000 – 1375 v. Chr.)

Ebenfalls auf der Insel Kreta fanden Forscher Tontafeln mit Symbolen und Schriften. Die Tafeln lassen sich nach ihrer Aufschrift in drei Gruppen einteilen. Die Tafeln der ersten Gruppe enthielten nur einzelne Symbole. Die Tafeln aus Gruppe zwei enthielten eine Schrift aus einfachen Linien, sie wurde daher Linear A genannt. Auf den Tafeln der dritten Gruppe war die vorherige Schrift verfeinert worden, sie bekam daher den Namen Linear B. Eine erfolgreiche Analyse der Schriften schien für die Tafeln der dritten Gruppe am wahrscheinlichsten, da man von dieser Art das meiste Material gefunden hatte. Die Tafeln enthielten eine Menge an Ziffern, sodass diese kein allzu großes Problem darstellten, bei den Schriftzeichen verhielt es sich dagegen anders. Die Forscher konnten nichts mit ihnen anfangen. Das einzige, was sie den Tafeln entlocken konnten war die Tatsache, dass sie offensichtlich von links nach rechts beschrieben worden waren, weil sich eine Lücke am Ende einer Zeile immer rechts und nie links befand und zweitens ließen sich 90 unterschiedliche Symbole identifizieren, was die Forscher glauben ließ, dass es sich um eine Silbenschrift und keine Buchstabenschrift handelte. Die Entdeckung von Linear B spaltete die Archäologen, da niemand wusste zu welcher Sprache diese Schrift gehörte. Die beiden Hauptrichtungen stritten zwischen minoisch und griechisch. Sir Arthur Evans, der die Tafeln entdeckt hatte, sollte das Ergebnis der Debatte nicht mehr miterleben. Die ersten Durchbrüche in der Analyse von Linear B erlangte die Professorin Alice Kober. Sie stellte fest, dass sich bestimmte Zeichengruppen an speziellen Positionen wiederholten und folgerte daraus, dass die Schrift zu einer beugenden Sprache gehörte, bei der sich Wortendungen verändern können. Darüber hinaus gelang es ihr sogar die Wortstämme und –endungen zu analysieren und sie fand heraus, dass dazwischen sogenannte Brückensilben standen, die mit einem Teil zum Wortstamm gehörten und mit dem zweiten Teil zur Endung. Daraus schloss sie, dass die Silben, die durch die Zeichen dargestellt wurden, jeweils einen Konsonanten gefolgt von einem Vokal darstellten. Die vollständige Entschlüsselung der Sprache blieb ihr allerdings aufgrund ihres frühen Todes verwehrt. Michael

[203] Pincock, Stephen / Frary, Mark: Geheime Codes, S. 20 f.
http://de.wikipedia.org/wiki/Diskos_von_Phaistos, letzter Zugriff: 21.03.2009.

Ventris trat Kobers Erbe bei der Entschlüsselung von Linear B an. Er ergänzte Kobers Arbeiten und entdeckte darüber hinaus Unregelmäßigkeiten, die ihn vermuten ließen, dass in Linear B stumme Vokale eingefügt wurden und dass die Schrift Zeichen für einzelne Vokale am Wortanfang bereithalten musste. Ventris schaffte es erste Wörter zu entschlüsseln und kam zu dem, für ihn erschreckenden, Ergebnis, dass es sich um eine alte Form der griechischen Sprache handeln musste, obwohl er selbst jahrelang fest überzeugt war, dass es eine eigene minoische Sprache sei. Als er seine ersten Ergebnisse vorstellte, bekam er in der weiteren Entschlüsselung der Zeichen Hilfe von einem Professor für griechische Philologie, John Chadwick. Gemeinsam gelang ihnen die komplette Entzifferung der Schrift Linear B.
Die ältere Schrift Linear A ist, obwohl sie Linear B ähnlich sieht, bis heute unentschlüsselt geblieben.[204]

2. Zur Renaissance

2.1. Die Rosenkreuzer (ca. 15. Jh. n. Chr.)

Zu den Anfängen des Rosenkreuzerbundes gibt es viele verschiedene Theorien. Die tatsächliche Entstehungsgeschichte konnte nie abschließend geklärt werden. Die Rosenkreuzer, oder genauer der „Orden der Gold- und Rosenkreuzer“, sind ein Geheimbund seit etwa Anfang des 15. Jh. Damals wurde ihnen vorgeworfen okkulte oder heidnische Rituale durchzuführen, dennoch wurde der Bund immer größer. Berichten aus den eigenen Reihen zufolge, mussten die Rosenkreuzer mit Verfolgungen, Übergriffen auf Niederlassungen und sozialer Ächtung kämpfen. Deshalb führten sie eine einfache Geheimschrift ein, um ihre Nachrichten zu verschlüsseln und somit ihre Mitglieder und Treffen zu schützen.[205]

2.2. Girolamo Cardano (16. Jh. n. Chr.)

[204] Singh, Simon: Geheime Botschaften, S. 266 ff.
[205] Wrixon, Fred: Geheimsprachen, S. 25.

Girolamo Cardano wurde 1501 in Pavia geboren. Cardano war zwar kein Universalgelehrter, dennoch beschäftigte er sich mit mehreren wissenschaftlichen Bereichen, hauptsächlich mit Medizin, Philosophie und Mathematik. Seine Leistungen in diesen Bereichen waren überragend. Es gelang ihm beispielsweise eine allgemeine Form zum Lösen kubischer Gleichungen zu finden. Cardanos mathematische Forschungen sind sicherlich von Bedeutung für die weitere Entwicklung der Kryptographie, sein persönliches kryptographisches Wirken war allerdings nicht so bedeutsam wie das seiner zuvor erwähnten Kollegen, dennoch trug auch Cardano seinen Teil zur polyalphabetischen Verschlüsselung bei, indem er den Klartext selbst als Schlüssel benutzte.[206]

2.3. Cabinet noir / die schwarze Kammer (ca. 16. Jh. n. Chr.)

Während der Renaissance in Italien kam es immer wieder zu Fehden rivalisierender Stadtstaaten. Dies brachte die Kryptographie deutlich voran, denn die Herrscher dieser Stadtstaaten waren darauf bedacht wirtschaftliche, diplomatische und militärische Informationen geheim zu halten. In dieser Phase begannen die Herrscher Venedigs Sekretäre einzustellen, die heimlich die Briefe an die Botschafter anderer Städte öffneten und deren Inhalt untersuchten. Dies versetzte Venedig über Jahrzehnte in Vorsprung gegenüber den übrigen Staaten. Als diese von der Methode Venedigs erfuhren, setzten Florenz, Genua und Neapel bald selbst Sekretäre zur Postüberwachung ein. Diese Büros, in denen der Postweg überwacht wurde, nennt man auch Cabinet noir oder schwarze Kammer. Da, in dem Wissen der Briefüberwachung, wichtige Informationen aber verschlüsselt wurde, mussten die Sekretäre in diesen schwarzen Kammern auch, zumindest grundlegende, kryptoanalytische Methoden beherrschen. Es handelt sich somit bei den schwarzen Kammern um eine der ersten großflächigen, professionellen kryptoanalytischen Einrichtungen.[207]

3. Zur Vorindustriellen Zeit

[206] http://seegras.discordia.ch/Essays/Krypto.txt, letzter Zugriff: 22.03.2009.
[207] Wrixon, Fred: Geheimsprachen, S. 28 f.

3.1. Karl I. und Sir John Wallis (17. Jh. n. Chr.)

Der spätere König Karl I. wurde im Jahre 1600 n. Chr. als Enkel der dreizehn Jahre zuvor hingerichteten Maria Stuart geboren. Er war zu Zeiten des englischen Bürgerkriegs König. Karl lieferte sich heftige Auseinandersetzungen mit dem englischen Parlament, außerdem formierte sich eine gegnerische Gruppierung zu Karls Ansichten, die „Puritaner“. Im August 1642 eskalierte der Konflikt und wurde zu einem bewaffneten Krieg. Die Puritaner sahen sich den Cavaliers, oder Royalisten, die treue Gefolgsleute von Karl waren, gegenüber in der Unterzahl, doch sie hatten den Taktiker Oliver Cromwell und den Mathematiker Sir John Wallis auf ihrer Seite. Wallis sollte später als der Vater der Kryptoanalyse in England bekannt werden. Cromwell erkannte Wallis‘ Begabung sehr schnell und ließ ihm sämtliche verschlüsselten Botschaften der Cavaliers überbringen, die die Puritaner abgefangen hatten. Dieser informationelle Vorteil versetzte Cromwell in die Lage den Krieg zu seinen Gunsten zu wenden. Im Juni 1645 gelang es den Puritanern eine Sammlung von Briefen der Royalisten zu erbeuten. Cromwell ließ sie zu Wallis bringen. Sie erhofften sich Informationen über weitere Pläne der Cavaliers. Tatsächlich handelte es sich dabei allerdings um Briefe von König Karl persönlich an seine Frau, in denen er ihr von Komplotten gegen das Parlament berichtete. Karl I. überführte sich damit selbst. 1649 wurde Karl, auf die gleiche Weise wie seine Großmutter Maria Stuart, hingerichtet.[208]

Während die Geschichte Karls I. damit endete, ging die von Sir John Wallis weiter. Über die Regentschaft der Puritaner hinaus arbeitete er als Kryptoanalytiker auch noch unter Karl II. und während der gemeinsamen Regentschaft von Wilhelm III. und Maria II. Ein weiterer großer Coup gelang ihm 1689, als er Briefe von Ludwig XIV. und dem französischen Botschafter in Polen entzifferte, in denen Ludwig ein Bündnis mit dem polnischen König plante um Preußen den Krieg zu erklären. Aus Angst vor einer politischen Großmacht auf dem europäischen Festland gab Wilhelm III. diese Informationen der Öffentlichkeit preis, mit den Auswirkungen, dass der Angriff auf Preußen fehlschlug, sämtliche Diplomaten aus Polen ausgewiesen wurden, Preußen noch militanter wurde und das Ansehen Ludwigs XIV. stark gelitten hatte.[209]

[208] Wrixon, Fred: Geheimsprachen, S. 33 f.
[209] Wrixon, Fred: Geheimsprachen, S. 36.

3.2. Die Kabinettskanzlei in Wien (17. – 18. Jh. n. Chr.)

Ende des 17. und Anfang des 18. Jahrhunderts kam es zu einer starken Verbreitung der schwarzen Kammern. Kryptoanalyse wurde professionell betrieben. Das versetzte der Kryptologie im Allgemeinen einen Schub, da im Kampf der Codemacher und Codeknacker jede Seite versuchte die Nase vorn zu haben. Die berühmteste schwarze Kammer war die geheime Kabinettskanzlei in Wien. Die Kabinettskanzlei versorgte die Herrscher Österreichs, allen voran Maria Theresia, die die Kabinettskanzlei eingeführt hatte, mit allen Informationen, die für sie wichtig waren. Sie galt als die Effektivste der schwarzen Kammern Mitte des 18. Jahrhunderts, doch ein korrupter Mitarbeiter stahl eine sorgfältige Auflistung der abgefangenen und entzifferten Briefe und verkaufte sie an den Sekretär der französischen Botschaft in Österreich, den Abbé Jean François Georgel, der sie Ludwig XV. zukommen ließ. Da sich unter den abgefangenen Briefen auch eigenhändig verfasste von König Ludwig befanden, traf dieser die Entscheidung in der Folgezeit die große Chiffre wieder vermehrt einzusetzen.

3.3. Die Freimaurer (17. Jh. n. Chr.)

Die Freimaurer gibt es noch heute. Sie zählen etwa fünf Millionen Mitglieder weltweit. Als offiziell anerkanntes Gründungsdatum gilt der 24. Juni 1717. Ihr Ursprung liegt aber fast 1000 Jahre früher. Die Freimaurer arbeiteten hauptsächlich an Großbauten wie Kirchen und Kathedralen seit dem 9 Jh. n. Chr. Sie schlossen sich zu Gilden zusammen. Diese Gilden hatten den Auftrag sich gegenseitig zu schützen und einen Qualitätsstandard zu gewährleisten.
Über die Freimaurer gibt es ganze Bücher, es ließe sich also eine Menge an Stoff hier zusammentragen. Eine kurze Suche über Google mit dem Stichwort „Freimaurer“ liefert auf die Schnelle über 700.000 Ergebnisse, doch die Weltanschauung, Rituale und Besonderheiten, sowie Ränge innerhalb der Logen sind nicht das Ziel dieser Arbeit. Doch auch die Freimaurer bedienten sich einer Geheimschrift. Es handelte sich dabei um eine einfache, monoalphabetische Ersetzung der Buchstaben durch bestimmte Zeichen. Die Einfachheit dieser Verschlüsselung lässt manche Kryptologen daran zweifeln, dass die Freimaurer

überhaupt ein Verschlüsselungsmotiv hatten, sie glauben, dass die abstrakten Zeichen eher dazu dienten den Bund geheimnisvoll erscheinen zu lassen.[210]

3.4. Der amerikanische Unabhängigkeitskrieg (18. Jh. n. Chr.)

Auch der amerikanische Unabhängigkeitskrieg trug seinen Teil zur Geschichte der Kryptographie bei, oder vielleicht sollte man besser sagen: Die Kryptographie trug ihren Teil zum amerikanischen Unabhängigkeitskrieg bei, denn es ist zwar nichts von der Entdeckung oder Entwicklung außergewöhnlicher Methoden während dieses Krieges bekannt, aber einige Schlachten und auch der Krieg im Gesamten wurden maßgeblich durch verschlüsselte Nachrichten beeinflusst. Der Niederländer Charles William Dumas, der mit den Kolonisten sympathisierte und später amerikanischer Geheimagent wurde, schlug Benjamin Franklin vor Spanien und Frankreich auf die Seite der Kolonien zu ziehen, außerdem nutzte er die Neutralität der Niederlande in diesem Krieg, sowie seine persönliche Freundschaft mit Kapitänen, um verschlüsselte Nachrichten zu transportieren. Dazu benutzte er Codewörter und eine alphanumerische Chiffre.
Während des Krieges gab es einige Doppelagenten, die ihre Stellung oder das in sie gesetzte Vertrauen ausnutzten, um mit geheimen Botschaften zu handeln.
Eine der wahrscheinlich bekanntesten Figuren dieses Krieges war Benedict Arnold, ein General der Kolonisten, der später desertierte und sich auf die Seite der Briten schlug. Arnold hatte das Kommando über den strategisch wichtigen Punkt Fort West Point. Diesen wollte er den Briten samt Außenposten und 3.000 Mann für ca. 20.000 britische Pfund verkaufen. Für die Verhandlungen mit den Briten nutzte er dabei eine Buch-Verschlüsselung. Aufgrund des Vertrauens, dass die Kolonisten ihm entgegen brachten, wurde seine Korrespondenz nie überwacht und die Briefe nicht entschlüsselt. Das Komplott konnte nur vereitelt werden, weil eine aufmerksame Patrouille der Kolonisten seinen Kontakt bei der britischen Armee, den jungen Major John André gefangen nahmen. André wurde gehängt, Arnold schlug sich zu den britischen Linien durch und schaffte es später auch dort in den Rang eines Generals. „Benedict Arnold“ gilt in den USA noch heute als Synonym für einen hinterhältigen Verbrecher.[211]

---

[210] Kippenhahn, Rudolf: Verschlüsselte Botschaften, S. 31 f.
[211] http://de.wikipedia.org/wiki/Benedict_Arnold, letzter Zugriff: 23.03.2009.
Wrixon, Fred: Geheimsprachen, S. 38 ff.

Drei der besten Kryptographen der Rebellen lebten in New York, das von den Briten beherrscht und in ein Armeelager verwandelt worden war: Benjamin Tallmadge, Robert Townsend und Samuel Woodhull. Sie sammelten in New York Informationen, die sie mit Hilfe einer Kombination aus unsichtbarer Tinte und einer Nomenklator-Verschlüsselung, sowie eines Buchcodes, für den ein Lexikon verwendet wurde, den Kolonisten übermittelten. Mit diesen Informationen gelang es General Washington New York so zu umstellen, dass der Befehlshaber Clinton mit seinen Truppen die Stadt nicht verlassen konnte und damit seine Kriegsführung von New York aus einschränken musste.
Im Herbst 1781 führte die Kryptoanalyse dazu, dass die Rebellen herausfanden, dass Lord Cornwallis seine Armee nach Yorktown verlegt hatte um dort auf Nachschub über den Seeweg zu warten. James Lovell entzifferte die abgefangenen Briefe mit fatalen Folgen für Cornwallis. Er musste kapitulieren, was den Sieg der Rebellen einleitete. Lovell fand außerdem heraus, dass die britischen Kryptographen immer die gleichen Geheimtextalphabete verwendeten. Sie änderten zwar ihre Chiffriermethoden, aber nur die Zuordnung der Symbole zu den Buchstaben des Klartextalphabetes in dem gleichen Geheimtextalphabet.[212]

3.5. Marie-Antoinette (18 Jh. n. Chr.)

Marie-Antoinette war die Tochter von Kaiserin Maria-Theresia von Österreich, Ehefrau des französischen Königs Ludwig XVI. und Schwester von Leopold II., Kaiser des Heiligen Römischen Reiches. Die Ehe zwischen Ludwig und Marie-Antoinette war alles andere als vorbildlich, sie gingen weitgehend getrennte Wege. Marie vergnügte sich mit Liebhabern. Die Korrespondenz mit diesen Liebhabern verschlüsselte sie mit einem System, das dem von Giovanni Porta sehr ähnlich war und mit einer, die aus dem Roman „Paul und Virginie“ abgeleitet war. Einer ihrer Liebhaber war der schwedische Graf Axel Fersen. Nachdem Ludwig und Marie aus Versailles flüchten mussten und Ludwig sich nicht mehr zu helfen wusste, nahm Marie das Ruder in die Hand. Sie versuchte mit Hilfe Fersens geheime Botschaften an die Anhänger in den zerstreuten Provinzen zu schicken und diese zu einen, damit sie dem König zur Seite standen. Außerdem sandte sie Botschaften an Freunde und Verwandte in ganz Europa. Das Verschlüsselungssystem, das sie dafür nutzte, war

[212] Wrixon, Fred: Geheimsprachen, S. 38 ff.

ein polyalphabetisches Substitutionsverfahren. Auch nachdem Ludwig einer neuen Verfassung zustimmte, blieb Marie-Antoinette weiterhin mit anderen Regierungen in Kontakt, doch ihre Chiffre wurde geknackt und die neue Regierung warf ihr und Ludwig Hochverrat vor. Beide wurden zum Tode verurteilt. Wieder einmal entschied die „Stärke“ einer Geheimschrift über das Schicksal.

3.6. Thomas Jefferson und Aaron Burr (18. – 19. Jh. n. Chr.)

Thomas Jefferson ist wohl am ehesten dafür bekannt, dass er der dritte Präsident der USA war, darüber hinaus war er aber auch noch der hauptsächliche Verfasser der Unabhängigkeitserklärung, Architekt, Erfinder und galt als Universalgelehrter. Auch für den Bereich der Kryptologie interessierte er sich. Jefferson erfand die sogenannte „Wheel Cypher“ oder „Jefferson-Walze“, die er selbst aber nie effektiv nutzte. Erst 120 Jahre später kam eine ähnliche Version der Walze bei der US-Armee zum Einsatz.[213]

Aaron Burr wurde 1800 mit Thomas Jefferson zusammen gewählt, Jefferson als Präsident, Burr als sein Vize-Präsident. Vier Jahre später bewarb sich Burr nicht mehr um das Amt, sondern als Gouverneur von New York. Doch sein Widersacher Alexander Hamilton brachte ihn öffentlich (und zu Unrecht) mit einer Verschwörung in Verbindung, sodass Burr die Wahl verlor. Burr wollte daraufhin Satisfaktion und forderte Hamilton zum Duell. Dieses fand auch statt und Hamilton wurde tödlich verletzt, dies führte aber zu einer öffentlichen Bestürzung und seine Freunde wandten sich von Burr ab. Er wurde in zwei Staaten wegen Mordes beschuldigt, stand aber nie deswegen vor Gericht. Daraufhin plante Burr eine Verschwörung. Er wollte mit ausländischen Geldern, einer Privatarmee, Land und Geheimschriften zum Verbergen seines Komplotts einen unabhängigen Staat im südlichen Teil der USA gründen. Sein Komplize James Wilkinson stellte sich allerdings selbst und übergab die Briefe Burrs, die mit einem Geheimtextalphabet aus John Enticks „New Spelling Dictionary“, sowie einer Symbolchiffre verschlüsselt waren, Thomas Jefferson. Dieser gab daraufhin den Befehl die Armee Burrs auszulösen und ihn selbst gefangen zu nehmen. Burr wurde wegen Hochverrats angeklagt. Trotz der Beweise durch die entschlüsselten Briefe, entschied der vorsitzende Richter John Marshall, dass es für Verrat mindestens zwei Zeugen geben müsse, die die Anklage nicht aufweisen

[213] Wrixon, Fred: Geheimsprachen, S. 47 f.
http://de.wikipedia.org/wiki/Jefferson-Walze, letzter Zugriff: 23.03.2009.

konnte. Infolgedessen wurde Aaron Burr aus Mangel an Beweisen freigesprochen. Er setzte sich in den folgenden Jahren nach Europa ab, bevor er nach New York zurückkehrte und bis zu seinem Tod im Jahre 1836 zurückgezogen lebte.[214]

4. Zum Industriezeitalter

4.1. Die Wahl des 19. US-Präsidenten (1876 n. Chr.)

1876 kam es zur umstrittensten Präsidentschaftswahl der Geschichte der USA. Samuel Tilden war Gouverneur von New York und Kandidat der Demokraten. Rutherford B. Hayes, Gouverneur von Ohio, war sein republikanischer Gegner. Nach der Auszählung der Stimmen hatten die Demokraten mit 184 Wahlmännerstimmen gewonnen, eine einzige zu wenig um Tilden direkt zum Präsidenten zu machen. In der Folge annullierten republikanisch geprägte Wahlbüros so viele demokratische Stimmen, dass Hayes zum Sieger erklärt werden konnte. Das entfachte einen Streit, der auf den Kongress überschwappte, wo sich ein republikanisch dominierter Senat und ein überwiegend demokratisch geprägtes Repräsentantenhaus gegenseitig in eine Pattsituation manövrierten. Um die Kontroverse zu klären wurde ein Ausschuss gebildet, der aus jeweils fünf Mitgliedern des Obersten Gerichtshofes, des Senats und des Repräsentantenhauses bestand. Doch auch dieser Ausschuss lieferte sich monatelang interne Kämpfe bis einer der Richter des Obersten Gerichtshofes von einem loyalen Republikaner abgelöst wurde, was zu einer Wahl nach Parteizugehörigkeit führte, die die Republikaner mit acht zu sieben Stimmen gewannen, damit wurde Rutherford B. Hayes zum 19. Präsidenten der USA. Die Demokraten fühlten sich betrogen. In welcher Weise Geheimschriften die Wahl beeinflussten wurde erst zwei Jahre später bekannt, als die New York Tribune im Sommer 1878 27 verschlüsselte Briefe abdruckte, die die Western Union einem Untersuchungsausschuss übergeben hatten und die republikanische Mitglieder an das republikanisch geprägte Blatt weitergaben. Das Verfahren, mit der die Briefe verschlüsselt worden waren, bestand aus einer Kombination von Transpositionen ganzer Wörter, einer lexikalisch gestützten Buchchiffre und einer monoalphabetischen Substitution. Dennoch gelang es drei Männern, John Hassard,

[214] Wrixon, Fred: Geheimsprachen, S.48 ff.
http://de.wikipedia.org/wiki/Aaron_Burr, letzter Zugriff: 23.03.2009.

William Grosvenor und Edward Holden, die Chiffre zu knacken. Das Ergebnis war ein herber Rückschlag für die Demokraten. Die Briefe enthielten Beweise, dass William Pelton, der Neffe des Demokraten Samuel Tilden, Stimmen für seinen Onkel gekauft hatte. Tildens Ansehen war ruiniert, obwohl er jede Beteiligung abstritt. In diesem Fall sorgte die Geheimschrift einerseits dafür, dass Tilden während des Wahlkampfes überhaupt eine Chance hatte Präsident zu werden, denn hätte Pelton die Briefe nicht verschlüsselt, wären seine Machenschaften sicher schon zu Zeiten des Wahlkampfes aufgeflogen und Tilden hätte jegliche Chance verloren, andererseits führten sie aber auch dazu, dass Tilden keine zweite Chance auf eine Kandidatur bekam.[215]

4.2. Indianerkriege (16. – 19. Jh. n. Chr.)

Seit der Entdeckung des amerikanischen Kontinents und der Besiedlung durch die Europäer kam es immer wieder zu Übergriffen und Kriegen zwischen den indianischen Ureinwohnern und den Kolonisten. Diese Kriege, die die Unterwerfung der Indianer zur Folge hatten, werden als Indianerkriege bezeichnet.
Nach dem amerikanischen Bürgerkrieg, der viele Menschen das Leben gekostet und ebenso viele Lebensgrundlagen zerstört hatte, zog es die Menschen Richtung Westen. Die Telegraphie und die Eisenbahn begünstigten Vorstöße in die Steppen des mittleren Westens, die zuvor weitgehend unkolonisiert verblieben und damit den sich zurückziehenden Indianern Lebensräume boten. Als nun die Kolonisten in dieses Land vorstießen, gerieten sie in Konflikte mit den dort lebenden Indianern und es kam in der Folge wieder vermehrt zu Kriegen zwischen den amerikanischen Ureinwohnern und den europäisch-stämmigen Kolonisten. Auch in diesen Kriegen spielten Signalsysteme eine große Rolle. Die Indianer verwandten Rauchzeichen zur Kommunikation über lange Wege in den Steppen, dabei gaben sie dem Feuer feuchtes brennbares Material bei (meistens nasses Gras oder Blätter), was zur Rauchentwicklung führte und deckten es anschließend ab. In bestimmten Abständen lüfteten sie dann die Decke, sodass der Rauch aufsteigen konnte, dabei ergab sich eine Kombination aus „Rauch“ und „Nicht-Rauch“ Signalen, die an den Morsecode erinnern. Die vorstoßenden Truppen der US Armee verwendeten ihre Winkersignale, sowie die Telegrafie, allerdings hatten sie damit einige Probleme, denn die

[215] Wrixon, Fred: Geheimsprachen, S. 64 ff.

Kommunikation mittels Winkertelegraphie war aufgrund von Wetter und Landfläche nicht immer uneingeschränkt möglich, zur Verwendung der Telegrafie musste hingegen zunächst Masten erbaut und Leitungen gezogen werden. In den Weiten der Steppe boten solche Masten aber ein leichtes Ziel für Übergriffe der Indianer, darum führte die Armee den Heliographen ein. Das Wort Heliograph kommt aus dem griechischen von „helios“ (die Sonne) und „graphein“ (schreiben). Mit Hilfe von Spiegeln konnte das Sonnenlicht so abgelenkt werden, dass man visuelle Signale verschicken konnte, außerdem eignete es sich um Morsezeichen visuell zu übertragen.[216]

4.3. Der Sezessionskrieg (1861 – 1865 n. Chr.)

Mitte des 19. Jh. kam es zum nächsten Krieg in den USA. Politische Spannungen, insbesondere durch die Sklavereifrage ausgelöst, hatten zu einer Spaltung der USA in die Union der Nordstaaten und die Konföderation der Südstaaten geführt. Eine entscheidende Rolle in diesem Krieg spielte die Telegrafie von der insbesondere die technisch weiter entwickelten Nordstaaten profitieren konnten. Die kryptographischen Methoden waren im Sezessionskrieg vielfältig, von Nomenklatoren über einfache Transpositionen, Caesar-Verfahren, sowie Buchchiffren bis hin zur Vigenère-Verschlüsselung, die die Südstaaten anwandten und die aufgrund von Übertragungsfehlern dazu führte, dass die eigenen Offiziere bei der Entschlüsselung oft mehr Probleme hatten, als die Kryptoanalytiker der Nordstaaten. Kryptographisch taten sich insbesondere zwei Personen hervor: Anson Stager und Albert Myer.[217]

4.3.1. Anson Stager (19. Jh. n. Chr.)

Anson Stager wurde 1825 geboren und war Mitbegründer der Western Union, sowie General der Unionsarmee im amerikanischen Bürgerkrieg. Während dieser Zeit entwickelte er ein Verschlüsselungssystem, das auf Transposition setzte und sich gut für die Verwendung mit der Telegrafie eignete. 1862 verwendeten sämtliche Unionstruppen die Stager-Chiffre.[218]

[216] Wrixon, Fred: Geheimsprachen, S. 66 f.
[217] Wrixon, Fred: Geheimsprachen, S. 55 ff.
[218] Wrixon, Fred: Geheimsprachen, S. 56.

4.3.2. Albert Myer und das wigwag-System (19. Jh. n. Chr.)

Albert James Myer wurde 1828 in Newburg geboren. Er war Chirurg und ebenfalls Offizier der Unionsarmee. Er war Kommandant der Fernmeldeeinheit und entwickelte ein Signalsystem für Flaggen, das er Flaggentelegraphie nannte. Das System funktioniert über die verschiedenen Flaggenstellungen, bzw. konkreter über die Winkel der Flaggen, die ihm später auch den Namen „wigwag“ bescherte. Es war der Vorläufer des noch heute bei Militärs eingesetzten Winkeralphabets. Das Winkeralphabet hatte im Sezessionskrieg den Vorteil, dass es von Spähern verwendet werden konnte, die sich einzeln vorwagten oder verschanzten und wichtige strategische Punkte auskundschafteten, die keine Anbindung an das Telegrafennetz hatten. Darüber hinaus ließ sich keine Leitung anzapfen und der Code abhören. Dafür hatte es den Nachteil, dass es ein visuelles Signalalphabet war, das theoretisch von jedem in der Nähe befindlichen Feind gesehen werden konnte, wenn man nicht vorsichtig war und sich seinen Platz vorher sorgfältig aussuchte. Obwohl Myer ein Offizier der Unionsarmee war, wurde das wigwag-System zum ersten Mal auf Seiten der Konföderierten eingesetzt, denn Myer hatte einen Assistenten, mit dem er an dem System arbeitete, Edward Alexander. Diesen zog es bei Kriegsbeginn aber auf die Seite der Südstaaten, wo er die erste Schlacht am Bull Run 1861 aufgrund des Flaggenalphabets für sich entscheiden konnte. Alexander hatte Aussichtsposten aufstellen lassen und diese mit den Flaggen versehen. Als sich ein Trupp der Unionsarmee näherte und einen Überraschungsangriff starten wollte, sah Alexander sie und gab diese Information mit Hilfe der Flaggen an Colonel Nathan Evans weiter, der den flankierenden Trupp mit Kanonen beschießen ließ, woraufhin diese sich zurückziehen mussten. Der Nachteil der Unionstruppen an diesem Tag war der, dass es Myer im Norden nicht gelungen war seine Vorgesetzten von seinem wigwag-System zu überzeugen, sodass es nicht eingesetzt wurde und die Unionstruppen die Nachricht, die Alexander an Evans sendete nicht verstehen konnte.

Ein Jahr später hatte Myer mehr Glück. 1862 rückte General Lee unbehelligt in die Unionsstaaten vor, bis eine seiner Nachschubeinheiten von einer Fernmeldeeinheit der Union entdeckt wurde. Die Nachricht wurde per Flaggensignal an die

---

http://en.wikipedia.org/wiki/Anson_Stager, letzter Zugriff: 24.03.2009.

Fernmeldezentrale in Point of Rocks durchgegeben, von wo aus sie über die Telegrafenlinie entlang der Bahnlinie von Baltimore nach Washington durchgegeben wurde. Die Union setzte zum Gegenangriff an und der Überraschungsangriff von General Lee und seinen Leuten war vereitelt.
Vom 1. – 3. Juli 1863 kam es zu einer entscheidenden Schlacht, die als Wendepunkt im amerikanischen Bürgerkrieg gilt: Die Schlacht von Gettysburg. Beide Seiten forderten per Signal Verstärkung an, sodass sich irgendwann 88.000 Soldaten der Nordstaaten und 73.000 Soldaten der Südstaaten gegenüberstanden. General Lee war ein gewiefter Stratege und wollte die Truppen der Union erneut flankieren, doch Späher der Union entdeckten die Truppenverbände am 2. Juli und gaben die Informationen weiter, was dazu führte, dass die Verteidigungslinie dort verstärkt wurde und die von der Flanke einfallende Armee abgewehrt werden konnte.
Am dritten Tag kam es schließlich zum letzten und entscheidenden Gefecht. General Lee wollte den Sieg erzwingen und fasste den Plan fast mit der gesamten Armee die Mitte der Unionslinie zu durchbrechen. Die Signalposten der Union wurden unter Beschuss genommen, um den Informationsweg zu durchbrechen. Da die Späher nun von ihren Flaggen keinen Gebrauch mehr machen konnten, schickten sie Boten zu der Fernmeldezentrale. Trotz des Beschusses gab Captain David Castle die Information über den massiven Angriff auf die Mittellinie mittels einer behelfsmäßigen Flagge an das Hauptquartier der Union weiter, so dass General Meade die Mitte verstärkte. Nur durch die schnelle und wagemutige Weitergabe der wichtigen Informationen konnte der Angriff abgewehrt werden.[219]

Abschließend lässt sich sagen, dass insbesondere die Telegrafie den Ausgang des Sezessionskrieges massiv mitbestimmte, da die so übertragenen Nachrichten schneller als jeder Bote waren. Vor allem die Unionsarmee konnte diesen Vorteil nutzen und sich oft auf Angriffe der Konföderierten vorbereiten, noch bevor diese sich in Marsch setzten. 1865 kapitulierte die Konföderation der Südstaaten.

5. Zum Ersten Weltkrieg (1914 – 1918 n. Chr.)

Wie in den meisten vorangegangenen Kriegen, spielte die Kryptologie auch im ersten Weltkrieg eine entscheidende und mitbestimmende Rolle. Am 28. Juli 1914 erklärte

[219] Wrixon, Fred: Geheimsprachen, S. 57 ff.

Österreich Serbien den Krieg, nachdem zuvor ein Serbe den österreichischen Thronfolger ermordet hatte. Die Zeit vor 1914 hatte in Europa zu Spannungen und Entfremdungen zwischen einzelnen Staaten geführt, sodass ein Großteil des europäischen Kontinents auf unterschiedlichen Seiten in den Krieg zog. Die alliierten Mächte bestanden aus Großbritannien, Frankreich, Russland, Serbien und Japan. Demgegenüber standen Deutschland, Österreich-Ungarn und später Bulgarien und die Türkei. Deutschland erklärte Russland und Frankreich den Krieg, sah sich aber in einem Zwei-Fronten-Krieg überfordert, sodass der nach Alfred von Schlieffen benannte Schlieffen-Plan umgesetzt wurde, der besagte, dass Deutschland so schnell wie möglich Frankreich einnehmen und in den Ostgebieten einen Verteidigungskrieg zur Haltung der Gebiete führen sollte. Da die deutschen Truppen die französischen Grenzlinien umgehen wollten und dabei durch das neutrale Belgien zogen, mischte sich Großbritannien in den Krieg ein, da England sich zum Schutz Belgiens verpflichtet hatte.

Wie stark die Kryptologie stets Kriege beeinflusst, erkennt man immer wieder an einzelnen Schlachten, deren Ausgänge direkt von Geheimschriften abhängten. So war es auch im August 1914, als Russland Westpreußen angriff. Da Deutschland dem Schlieffen-Plan gefolgt war, war Preußen nur zur Verteidigung militarisiert. Die übrigen Truppenverbände waren für den Angriffskrieg gegen Frankreich abgezogen worden und so waren die russischen Truppen den Preußischen klar überlegen. Doch die Russen hatten ein Problem: ihre kryptologische Kriegsvorbereitung war nicht sorgfältig genug gewesen und so besaßen sie nicht genügend Chiffren um sämtliche Nachrichten zu verschlüsseln, was dazu führte, dass sie einige von ihnen in Klartext abfassen mussten. Da die Deutschen die Funkwege der Russen abhörten, waren sie über einen Großteil der Bewegungen und Strategien informiert und konnten sich darauf vorbereiten. Trotz zahlenmäßiger Überlegenheit kassierten die russischen Truppen eine vernichtende Niederlage.

Russland war jedoch nicht die einzige alliierte Macht gewesen, die sich kryptologisch nicht ausreichend auf den Krieg vorbereitet hatte. Zu Kriegsbeginn waren die Alliierten allgemein kryptologisch ins Hintertreffen geraten. Ebenfalls im August 1914 erhielt das deutsche Kriegsschiff Goeben den Auftrag russische Häfen zu beschießen, die am schwarzen Meer gelegen waren. Die Alliierten konnten zwar Funksprüche des Schlachtkreuzers abfangen, doch bis sie die Nachrichten entschlüsselt hatten war es bereits zu spät und sie konnten den Angriff nicht mehr

abwehren. Das führte dazu, dass die Türkei auf Seiten Deutschlands und Österreich-Ungarns in den Krieg zog.[220]

5.1. Sektion 25 / Room 40

Die Probleme beim Entschlüsseln der Botschaften, die im Ergebnis dazu geführt hatten, dass die Alliierten sich nun mit der Türkei einem weiteren Feind gegenüber stehend sahen, führten dazu, dass das englische Parlament eine Abteilung einrichtete, die sich ausschließlich mit Kryptologie auseinandersetzte. Der offizielle Name dieser Abteilung war „Sektion 25“, doch allgemein wurde sie nach dem Raum in dem sich diese Abteilung befand „Room 40“ benannt. Room 40 avancierte zum wichtigsten Kryptoanalyse-Dienst der Allianz. Im September 1914 konnte die russische Marine aus der zuvor auf Grund gelaufenen Magdeburg zwei Codebücher bergen. Diese wurden an Room 40 weitergeleitet und tatsächlich gelang es den Kryptoanalytikern der Abteilung den Code zu knacken. Sie fanden heraus, dass die Codewörter selbst verschlüsselt worden waren. Im Dezember erhielt Room 40 ein weiteres Codebuch von einem deutschen Schiff und fügte es den Magdeburg-Akten bei. Mit diesem Material war es Room 40 zunächst rückwirkend möglich gewesen Funksprüche der Magdeburg zu entschlüsseln. Im Januar 1915 machte sich der Eifer der Agenten aber schließlich vollends bezahlt, als es ihnen gelang eine wichtige Nachricht der deutschen Marine zu entschlüsseln, die besagt, dass sich die Schiffe, die die englischen Küstenorte beschossen am 16. Januar auf der Doggerbank treffen sollten. Die britische Admiralität reagierte sofort und entsandte eigene Kriegsschiffe dorthin, die schließlich einen Sieg auf der Doggerbank errangen.

Der wahrscheinlich größte Erfolg gelang Room 40 im Oktober 1916 und war der Auslöser dafür, dass die zuvor neutralen USA am 6. April 1917 auf Seiten der alliierten Mächte in den Krieg zog. Bereits 1914 hatten die Briten das transatlantische Kabel der Deutschen gekappt, sodass die für ihre Korrespondenz mit dem amerikanischen Kontinent andere Kabel nutzen mussten. Da sich die USA neutral verhalten und die diplomatischen Beziehungen mit Deutschland aufrechterhalten wollten, boten sie ihr Kabel an, das von Berlin über Kopenhagen nach London und von dort schließlich über den Atlantik führte. Im Januar 1917 nutzte der deutsche Außenminister Arthur Zimmermann diese Verbindung, um dem deutschen

[220] Wrixon, Fred: Geheimsprachen, S. 67 f.

Botschafter in Washington, Graf Johann von Bernstorff, eine Nachricht zukommen zu lassen, der diese dann an den Botschafter in Mexico City, Heinrich von Eckardt, weiterleiten sollte. Die Briten fingen dieses Telegramm allerdings ab und es gelang ihnen, die Verschlüsselung zu brechen. Das Telegramm beinhaltete Informationen darüber, dass die Deutschland einen umfassenden U-Boot-Krieg plante, auch gegen neutrale Schiffe. In der Angst, dass dies dazu führen würde, dass sich die USA in den Krieg einmischten, schlugen sie ein Bündnis mit Mexico vor. Mexico sollte den USA den Krieg erklären, um sie davon abzuhalten am Krieg in Europa teilzunehmen. Dafür sollte Mexico finanzielle Unterstützung, sowie die in einem vorangegangenen Krieg an die USA verlorenen Territorien Texas, Arizona und New Mexico erhalten. Das Telegramm wurde veröffentlich und führte im Ergebnis dazu, dass die USA ihren neutralen Status aufgaben.[221]

5.2. Der österreichische Geheimdienst

Auch auf Seiten der Mittelmächte wurde die Kriegsführung mit kryptologischen Mitteln beeinflusst. Österreich unterhielt während des Ersten Weltkrieges einen Geheimdienst, der sich intensiv mit der Kryptoanalyse feindlicher Nachrichten befasste. Insbesondere an der Südfront gegen Italien versetzte sie das in eine komfortable Lage. Italien hatte 1915 die Seiten gewechselt und kämpfte nun gemeinsam mit den alliierten Mächten. Dem Chef des österreichischen Nachrichtendienstes war es aber vor Kriegsbeginn gelungen eine Kopie der „cifrario rosso“ (zu Deutsch: rote Chiffre) zu kaufen, die das italienische Militär verwandte. Dadurch konnte Österreich seine Kriegsführung gegen Italien umfassend planen. Erst zwei Jahre später, im Herbst 1917 bemerkten die Italiener, dass ihre Botschaften abgefangen und entschlüsselt wurden und sie änderten ihre Kryptographiemethoden.[222]

5.3. Der Fall Mata Hari

Mata Hari zählt wohl zu den bekanntesten Persönlichkeiten des ersten Weltkrieges. Sie wurde 1876 in Leeuwarden in den Niederlanden als Margaretha Geertruida Zelle geboren. Schon vor dem ersten Weltkrieg war sie als exotische Tänzerin berühmt.

[221] Wrixon, Fred: Geheimsprachen, S. 68 ff.
[222] Wrixon, Fred: Geheimsprachen, S. 72.

Als der Krieg schließlich ausbrach wurde sie von den Deutschen als Geheimagentin angeworben. Sie erhielt den Decknamen H-21. Um Informationen für die Deutschen zu sammeln ging sie Liebesbeziehungen mit französischen und spanischen Offizieren ein. Im Dezember 1916 entschlüsselten die Kryptoanalytiker von Room 40 Nachrichten, die über das Kabel Berlin-Madrid übertragen wurden und Geld, sowie neue Einsatzbefehle für Agent H-21 anordneten. Daraufhin wurde Mata Hari in Frankreich verhaftet und wegen Doppelspionage und Hochverrat zum Tode verurteilt. Das Urteil wurde 15. Oktober 1917 vollstreckt. Im Januar 1999 gab der britische Geheimdienst Akten aus der Zeit des ersten Weltkrieges über Mata Hari frei, die angeben, dass Mata Hari den Deutschen keine bedeutsamen Informationen liefern konnte. 2017, einhundert Jahre nach der Hinrichtung Mata Haris, sollen die französischen Gerichtsakten veröffentlich werden, die vielleicht mehr Licht ins Dunkel um den Mythos Mata Hari bringen.[223]

5.4. Die A.E.F. und Codebücher in Massen

Die Truppen der American Expeditionary Force (A.E.F.) waren die ersten amerikanischen Einheiten, die den europäischen Kontinent erreichten, nachdem die USA in den Krieg eingetreten war. Die Einheiten nutzten zur Kommunikation Funk, Telefon oder den Postweg. Aus der eigenen Geschichte hatten die Amerikaner gelernt wie wichtig eine starke Verschlüsselung der Kommunikation im Feld war und so wurde die „Code Compilation Section“ eingerichtet, die in der Folge zunächst zwei Codebücher für den Einsatz im Feld verfasste: „The American Trench Code“ und den „Front-Line Code“. Doch beide Codes waren zu schwach und wurden schnell geknackt, hinzu kam, dass ihr Einsatz an der Front zu zeitaufwändig war. Etwa ein halbes Jahr später, im Sommer 1918, wurden die Codebücher durch eine Reihe neuer Bücher ersetzt, die den Namen „River Codes“ erhielten und aus sieben einzelnen Codebüchern bestanden: „Potomac“, „Suwannee“, „Wabash“, „Mohawk“, „Alleghenny“, „Hudson“ und „Colorado“. Diese Codes hatten den Vorteil, dass sie schnell ausgetauscht werden konnten, wenn eines der Codebücher in die Hände der Feinde fiel. Eine zweite Armee erhielt darüber hinaus andere Codebücher:

[223] Wrixon, Fred: Geheimsprachen, S. 72 f.
http://de.wikipedia.org/wiki/Mata_Hari, letzter Zugriff: 25.03.2009.

„Champlain“, „Huron“, „Osage“ und „Seneca“, die den Namen „Lake Series“ erhielt und mit einer „Emergency Code List“ abgesichert war.[224]

5.5. One-Time-Pads

Das One-Time-Pad (deutsch: Einmal-Block) bezeichnet ein polyalphabetisches Verfahren, bei dem der Schlüssel mindestens so lang ist wie die Nachricht selbst, sodass es keine Schleifen gibt und bei dem jeder Schlüssel nur einmal verwendet wird. Damit ist das One-Time-Pad ein absolut sicheres Verfahren, solange es nicht durch Unachtsamkeit zu einer zufälligen Wiederholungsfolge kommt. Die Idee dazu hatte der Amerikaner Gilbert Vernam bereits 1918. Joseph Mauborgne, dem 1914 ein erster kryptologischer Durchbruch mit der Entschlüsselung der Playfair-Chiffre gelungen war, bemerkte allerdings, dass Vernams noch nicht ganz ausgereiftes Verfahren zu einer Wiederholung des Schlüssels führen könnte, wodurch das Verfahren angreifbar war, also kombinierte er es mit dem nichtperiodischen Schlüssel des Army Signal Corps, dadurch waren zufällige Wiederholungen ausgeschlossen und das Verfahren unangreifbar. Das One-Time-Pad wird noch heute zur Verschlüsselung verwendet.[225]

6. Die Zeit zwischen dem Ersten und Zweiten Weltkrieg (1918 – 1939 n. Chr.)

6.1. Die schwarze Kammer der USA

Als die USA 1917 in den Ersten Weltkrieg eintraten, hatten sie im militärischen Geheimdienst eine Abteilung eingerichtet die sich mit Kryptoanalyse befasste. Diese Abteilung bekam den Namen MI-8 und konnte in den letzten beiden Kriegsjahren einige Erfolge verbuchen. Nachdem der Konflikt in Europa 1918 beendet war, fürchtete der Leiter des MI-8, dass die Maxime des Informationsvorsprunges durch Kryptographie in Vergessenheit geraten würde, also wandte er sich an den amerikanischen Außenminister Frank Polk. Gemeinsam richteten sie eine neue MI-8 ein, die in Anlehnung an die schwarzen Kammern der Renaissance eben jenen

[224] Wrixon, Fred: Geheimsprachen, S. 73 f.
[225] Wrixon, Fred: Geheimsprachen, S. 610 f.

Spitznamen bekam. Yardley nutzte diese Einrichtung zur Überwachung der Korrespondenz von ausländischen Botschaftern, aber auch Firmen um einen wirtschaftlichen Vorteil zu erringen. Die Abteilung brachte der amerikanischen Außenpolitik immense Vorteile, so war es Yardleys Männern beispielsweise gelungen eine wichtige japanische Geheimschrift zu knacken, die den Namen kata kana trug und für diplomatische Zwecke eingesetzt wurde. Auf einer Abrüstungskonferenz in Washington im November 1921, wurden sämtliche Nachrichten abgefangen, die der japanischen Delegation übermittelt wurde. Sämtliche Schachzüge und Verhandlungspositionen der Japaner lagen damit offen und die Vertreter der USA konnten sie unter Druck setzen.[226]

6.2. Das Buch „the american black chamber"

1928 erhielt die schwarze Kammer der USA ihren Todesstoß. Herbert Hoover wurde zum Präsident gewählt und vertrat ein Saubermann-Image. Funkaufklärung und Kryptographie wurden als unmoralisch gescholten. Als sein Innenminister Henry Stimson erfuhr, dass die schwarze Kammer vom Innenministerium gestützt wurde, strich er ihnen kurzerhand die finanziellen Mittel, sodass die Kammer ihre Arbeit aufgeben musste. Verbittert über diese Entwicklung schrieb der ehemalige Leiter Herbert Yardley das Buch „the american black chamber", in dem er die Erfolge der schwarzen Kammer und deren Folgen aufzeigte, um die Amerikaner auf die Gefahr einer schlechten Kryptographie-Politik hinzuweisen. Beim Volk und den Kritikern gingen die Meinungen über dieses Werk auseinander. Kryptologen hingegen befürchteten einen irreparablen Schaden für die Geheimdienste der USA. Tatsächlich sorgte das Buch in Japan für einen Eklat, weil Yardley die Brechung der diplomatischen kata kana – Chiffre, sowie die Vorteile der USA während der Abrüstungskonferenz niedergeschrieben hatte. Japan ließ darauf hin bei der Verschlüsselung und Übermittlung von Botschaften besondere Sorgfalt walten.[227]

6.3. Die japanische Tokumu Han

[226] Wrixon, Fred: Geheimsprachen, S. 75 ff.
[227] Wrixon, Fred: Geheimsprachen, S. 79 f.

Die Tokumu Han war eine, von den Japanern 1925 eingeführte, Kryptoanalyseabteilung. Sie war der Trumpf auf Seiten der Japaner während der Mandschurai-Krise im Vorfeld des zweiten Japanisch-Chinesischen Krieges. Der Tokumu Han gelang es den Gray Code, den die USA für ihre ausländischen Botschaften verwendeten, zu knacken. Die Chinesen verwendeten eine sehr ähnliche Methode was dazu führte, dass die Japaner mittels des Gray Code in der Lage waren Informationen über einige militärische Schläge abzufangen und zu entschlüsseln. So fanden sie heraus, dass die Chinesen einen Luftangriff planten, die Japaner reagierten sofort, mobilisierten ihre eigenen Maschinen und bombardierten den Flugplatz auf dem die chinesischen Flugzeuge wehrlos standen. Fast alle chinesischen Flugzeuge wurden bei diesem Angriff zerstört.[228]

6.4. Die ECM und Rückkehr zur Streifen-Chiffre

Die ECM oder Electronic Code Machine war eine Chiffriermaschine die mit Walzen arbeitete und von den Marinestreitkräften der USA eingesetzt wurde. Da die Japaner bereits ähnlich arbeitende Maschinen intensiv untersucht hatten, fiel es ihnen nicht schwer die Verschlüsselung der ECM zu knacken. Taktische Bewegungen der Japaner führten dazu, dass die USA bald bemerkten, dass ihr System gebrochen und ihre Nachrichten nicht mehr geheim waren. Daher verzichteten sie auf den Einsatz der ECM und verwendeten in der Folgezeit wieder eine Streifen-Chiffre. Streifen-Chiffren sind polyalphabetische Substitutionen aus mehreren Verschlüsselungsalphabeten, die gegeneinander verschoben werden können. Es gab mehrere solcher Systeme bei der US Armee, darunter die CSP 642 mit 30 Alphabetstreifen, die dadurch variiert wurden, dass nicht immer alle 30 Streifen verwendet wurden. Die M-138-A hatte sogar 100 Streifen, von denen aber immer nur höchstens 30 gleichzeitig verwendet wurden. Das steigerte die möglichen Kombinationen und damit die Effektivität des Verfahrens allerdings deutlich.[229]

7. Zum zweiten Weltkrieg

[228] Wrixon, Fred: Geheimsprachen, S. 80 f.
[229] Wrixon, Fred: Geheimsprachen, S. 81 f.

7.1. Copek

Auch auf Seiten der Alliierten wurden verschiedene Geheimschriften verwendet. Eines davon war Copek. Das Misstrauen der USA gegenüber Japan hatte dazu geführt, dass die Vereinigten Staaten in der Zeit nach dem Ersten Weltkrieg zur Überwachung des pazifischen Raums spezielle Aufklärertruppen gebildet hatten, die an unterschiedlichen Positionen Stellung bezogen, da die USA mehr Leute brauchten, die den kata kana Code der Japaner verstehen konnten. Insgesamt 176 handverlesene Soldaten wurden einem Spezialtraining in einem Blockhaus auf dem Dach des Marineministeriums unterzogen, dieser ungewöhnliche Ort brachte ihnen den Namen „On-The-Roof-Gang“ ein. Nach Abschluss des Lehrganges bezogen sie ihre Stellungen auf den Philippinen, Hawaii, in Alaska oder auf Bainbridge bei Seattle. Das Hauptquartier aber befand sich in Washington D.C.
Zur Kommunikation zwischen diesen Außenposten und der Zentrale Station Negat in Washington wurde Copek eingesetzt. Copek funktionierte ähnlich wie die Enigma mittels elektrischer Rotoren. Da es nicht so oft eingesetzt wurde wie die Enigma fehlte den Angreifern oftmals einfach genügend chiffrierter Text um die Verschlüsselung zu brechen, sodass Copek relativ sicher war.[230]

7.2. Purple

Purple war ein japanisches Chiffrierverfahren während des zweiten Weltkriegs gewesen. Die Japaner waren nach den Enthüllungen Yardleys in „the american black chamber“ vorsichtig geworden und hatten zunächst eine Chiffriermaschine gebaut, die von den amerikanischen Militärs den Codenamen Red erhalten hatte. Tatsächlich war es den Kryptoanalytikern der USA auch gelungen Red zu knacken, doch der Erfolg währte nicht lange, denn bald darauf entzifferten sie die letzte Red-Nachricht. Die Botschaft besagt, dass man auf eine weiterentwickelte Chiffriermaschine umsteigen würde, die Alphabet-Schreibmaschine ‘97. Diese erhielt, ebenfalls von den Amerikanern, den Codenamen Purple.
Purple beruhte auf einer polyalphabetischen Substitution und konnte hunderttausende solcher Substitutionsalphabete erzeugen. Dieser Code stellte die U.S. Kryptoanalytiker vor Probleme. Der bedeutendste unter ihnen war William

[230] Wrixon, Fred: Geheimsprachen, S. 78, S. 84 f.
http://www.usncva.org/history.shtml, letzter Zugriff: 25.03.2009.

Friedman. Friedman hatte keine Pläne über die Purple zur Verfügung wie die Briten, Franzosen und Polen diese über die Enigma hatten, dennoch gelang es ihm und seinem Team aus den Aufklärungsarbeiten von Yardleys schwarzer Kammer Gewohnheiten der Japaner, wie z.B. Anrede oder Grußformel, zu analysieren und mit dem Purple-Code in Verbindung zu bringen. Im Herbst 1940 hatten sie ohne Kenntnis der Originalmaschine eine Purple nachgebaut und ab 1942 war diese Maschine so ausgereift, dass die USA fast alle japanischen Nachrichten mitlesen konnten. William Friedman gilt als einer der größten Kryptoanalytiker aller Zeiten, außerdem zählt das Brechen der Purple-Chiffre, ohne Kenntnis über die Maschine selbst, zu den bedeutendsten Kryptoanalyse-Erfolgen der Geschichte.[231]

7.3. Pearl Harbor

Eine der wohl berühmtesten Schlachten des Zweiten Weltkriegs war die bei Pearl Harbor, als Japan einen Luftangriff auf die im Hafen vor Anker liegende Pazifikflotte der USA ausführte. Der Angriff auf Pearl Harbor leitete die Wende im Zweiten Weltkrieg ein, da er Auslöser dafür war, dass die USA aktiv wurden. Doch wie kam es zum Angriff auf Pearl Harbor?

Vor Beginn des Zweiten Weltkriegs befand sich Japan bereits mit China im Krieg, den Japan weitgehend dominierte. Im Verlauf dieses Krieges wechselten die USA ihre Stellung, waren sie zunächst neutral gewesen, sympathisierten sie immer mehr mit China, ohne diese im Krieg zu unterstützen. Anfang des Jahres 1940 war der Erste Weltkrieg im Gange, doch die USA hielten sich zurück, allerdings befürchteten sie, dass Japan in Französisch-Indochina einmarschieren würde, also schickten sie eine offizielle Warnung an Japan heraus dies zu unterlassen und verlagerten ihre Pazifikflotte demonstrativ von San Diego nach Pearl Harbor. Japan ließ sich davon nicht beeindrucken. Im Juli 1940 zogen militärische Einheiten der Japaner in Französisch-Indochina ein. Daraufhin verhängten die USA ein Öl-Embargo gegen Japan. Großbritannien und Niederländisch-Indien schlossen sich an, so verlor Japan 75% seines Außenhandels und 90% seiner Öl-Importe. Japan musste reagieren. Sie konnten entweder mit den USA in Verhandlungen treten, um die Aufhebung des Embargos zu erwirken und damit Zugeständnisse machen und weiterhin von Öl-Importen abhängig zu sein, oder sie konnten die südlichen Kolonien Großbritanniens

[231] Wrixon, Fred: Geheimsprachen, S. 85 ff.
Schmeh, Klaus: Kryptographie, S. 676 ff.

und der Niederlande angreifen, um sich selbst mit Öl zu versorgen. Japan entschied sich für den zweiten Weg, obwohl sie dennoch zunächst mit den USA in Verhandlungen traten. Das Problem war nämlich, dass zwischen Japan und den Kolonien, die sie erobern wollten, noch die Philippinen lagen. An dieser Stelle hätten die USA bei einem eventuellen Krieg die Nachschubwege Chinas unterbrechen können. Am 7. Dezember überreichte Japan den USA die Erklärung, dass sie keinen Sinn in weiterführenden Verhandlungen sehen und diese daher abbrechen würden. Zeitgleich sollte ein Überraschungsangriff auf Pearl Harbor stattfinden. Wegen Fehler und Schwierigkeiten bei der Nachrichtenübermittlung von Tokio nach Washington, erreichte die Botschaft über die Einstellung der Verhandlungen Washington erst einige Stunden nach dem Angriff auf Pearl Harbor.

Doch was war mit der Funkaufklärung geschehen? Gab es keine Anzeichen für den Angriff auf Pearl Harbor? Ein Problem der „On-The-Roof-Gang“, die den pazifischen Raum überwachte, war, dass sie feste Einsatzgebiete hatte. Darunter ist nicht etwa eine territoriale Einteilung zu verstehen, sondern vielmehr eine Aufgabenspezifische. Das Team auf Hawaii befasste sich mit dem Funk der japanischen Admiralität, während die auf den Philippinen stationierte Einheit sich dem wichtigen Marinesystem „JN25“ widmete. Aus einer Übervorsicht heraus und um den Fokus auf den eigentlichen Aufgaben zu halten, hatten die einzelnen Stationen keine Schlüssel der für die Chiffren, mit denen sich die jeweils anderen Stationen befassten. Wie sich später herausstellte war das insbesondere für die Truppe auf Hawaii ein großer Nachteil gewesen, denn obwohl sich dort ein japanisches Konsulat befand, konnte die Einheit die Nachrichten nicht entschlüsseln, weil sie die dafür nötigen Schlüssel nicht hatten. Hinzu kam, dass einige hochrangige Offiziere die Entscheidung getroffen hatten, nicht alle Nachrichten, die entschlüsselt werden konnten an alle Außenposten weiterzugeben. Von dieser Entscheidung waren zwei Kommandeure in Pearl Harbor betroffen: Admiral Husband Kimmel und General Walter Short. Den USA unterlief ein weiterer Fauxpas, die Japanologin Dorothy Edgers war wegen ihrer Vertrautheit mit der japanischen Sprache in der Dechiffrierungsabteilung in Washington eingesetzt worden. Sie bemerkte in einigen Nachrichten des japanischen Konsuls auf Hawaii an Tokio, dass ein Spion in Pearl Harbor postiert war, der per Lichtsignal an ein japanisches U-Boot genaue Informationen über die im Hafen liegende Flotte sendete. Edgers benötigte für die Entschlüsselung bis tief in die Nacht, sodass ihr Vorgesetzter bereits im Feierabend war. Sie legte ihm die

entschlüsselten Briefe auf den Schreibtisch, doch am nächsten Morgen war es bereits zu spät, es war der 7. Dezember 1941 und der Angriff auf Pearl Harbor hatte begonnen.
Der Kriegseintritt der USA wurde von einer massiven militärischen Aufrüstung begleitet, dies umfasste neben Kriegsmaschinen, Gewehren und Soldaten vor allem auch die Kryptoanalyse-Abteilung.[232]

7.4. Der B-Dienst und die Wolfsrudel

Da im zweiten Weltkrieg beide Seiten mit Chiffren arbeiteten, hatten nicht nur die Alliierten Kryptoanalytiker am Werk, sondern auch die Deutschen. Eine dieser Gruppen gehörte der Marine an und wurde von ihrem Befehlshaber, Admiral Dönitz, Beobachtungs-Dienst, oder kurz B-Dienst, genannt. Dieser Dienst knackte eine große Anzahl an britischen Codes, sodass die Marine Kenntnis der Lage und Wege britischer Versorgungsschiffe und Konvois hatte. Diese Informationen gaben sie an die „Wolfsrudel“ weiter. Als Wolfsrudel wurden im Zweiten Weltkrieg die U-Boot-Truppen der Nazis bezeichnet. Während die Alliierten ihre Schiffe vor gefährlichen Gebieten warnten, informierten sie den B-Dienst gleichzeitig über die neue Route der Schiffe. Die Wolfsrudel rückten an und zerstörten die Schiffe. Mit Hilfe der Arbeit des B-Dienstes gelang es den Nazis ihre deutlich unterlegene Marine aus aussichtslosen Kämpfen herauszuhalten und der gegnerischen Armada immer wieder deutliche Rückschläge zuzufügen.
Im Frühjahr 1940 plante Hitler den Norwegenfeldzug. Dies war auch den Alliierten nicht verborgen geblieben und so planten sie den Hafen von Narvik zu verminen, um die deutsche Marine zu schwächen. Dem B-Dienst gelang es allerdings einige britische Codes zu brechen und gelangte damit an die Information. Die Deutschen landeten daraufhin nicht in Narvik, sondern führten nur einen Scheinangriff durch und setzten ihre Landungstruppen an anderen Orten ab. Der B-Dienst brachte den Nazis viele Erfolge während des Zweiten Weltkrieges ein, doch die Alliierten änderten ihre Taktik gegen die Wolfsrudel und verbesserten ihre Verschlüsselungsmethoden, gleichzeitig gelang es ihnen immer häufiger die Chiffren der Deutschen zu knacken, sodass sie bald wieder die Oberhand gewannen.[233]

---

[232] Wrixon, Fred: Geheimsprachen, S. 84 ff.
http://de.wikipedia.org/wiki/Angriff_auf_Pearl_Harbor, letzter Zugriff: 25.03.2009.
[233] Wrixon, Fred: Geheimsprachen, S. 89 ff.

7.5. Die Schlacht um Midway

Die Schlacht um Midway war ein Siegeszug der amerikanischen Kryptologie gewesen. Im Juni 1942 wollten die Japaner die Midway Islands sowie einige strategisch wichtige Punkte auf den Aleuten besetzen und dabei die Pazifikflotte der Amerikaner vernichten um ihnen anschließend eine Friedenskonferenz aufzuzwingen. Die Funksprüche wurden mit dem japanischen „JN25“-Code verschlüsselt. Die Analyse der Funksprüche stieß die Kryptoanalytiker auf die immer wiederkehrende Folge „AF“. Aus der Vergangenheit wussten sie, dass die Japaner solche Kürzel für Ziele, Punkte oder Positionen verwendeten, so stand „AK“ beispielsweise für Pearl Harbor. Die USA hatten die richtige Vermutung, dass „AF“ für die Midway Inseln stand, sicher waren sie sich aber nicht. Zur Überprüfung ihrer Vermutung schmiedeten sie einen Plan. Sie wiesen das Midway-Hauptquartier an eine Meldung herauszugeben, nach der die Anlage zur Wasserdestillierung defekt sei. Der Plan ging auf. Die Japaner hatten die Meldung abgehört und bei der Übermittlung der Nachricht für Midway erneut das Kürzel „AF“ eingesetzt. Das anschließende Abwehrmanöver basierte auf einer Täuschung der japanischen Marine. Während fast die gesamte noch funktionsfähige Pazifikflotte der USA sich auf den Weg nach Midway machte, funkten der Kreuzer Salt Lake City im Korallenmeer und das Begleitschiff Tangier bei den Neuen Hebriden, Nachrichten hin und her, wie sie normalerweise für die Kommunikation zwischen Flugzeugträgern und ihren Flugzeugen verwendet wurden. In der Annahme, die Pazifikflotte befinde sich noch im Korallenmeer, führten die Japaner ihre Angriffe durch. Von den Einheiten der U.S. Navy überrascht, verloren sie in den Kriegstagen vom 3. bis 6. Juni 1942 einen Großteil ihrer Flotte.[234]

7.6. D-Day (Die Landung der Alliierten in der Normandie)

Am 6. Juni 1944 begann die Landung der Alliierten Streitkräfte in der Normandie um die Nazis zurückzuschlagen. Dieses Datum wird auch als D-Day bezeichnet. Die Landung gehörte zur Operation Overlord, die zum Ziel hatte die Deutschen aus Nordfrankreich zu vertreiben. Zur Geheimhaltung der Pläne von Operation Overlord

[234] Wrixon, Fred: Geheimsprachen, S. 94 ff.

planten die Alliierten ein umfangreiches Täuschungsmanöver, ähnlich dem in der Schlacht um Midway, mit dem Namen Operation Fortitude. Unter dem Codenamen Skye wurden eine britische Armee bestehend aus 350.000 Mann, sowie ein 15. U.S.-Corps und russische Truppenverbände erfunden, die sich in Schottland formierten, um einen Angriff auf Norwegen vorzubereiten. Hintergrund war, dass man die Divisionen der Nazis an dieser Stelle blockieren wollte, sodass sie nicht in die Normandie abgezogen werden konnten. Den Codenamen Quicksilver bekam ein Ablenkungsmanöver, das eine weitere amerikanische Armee erfand, die Calais angreifen sollte. Dort war die 15. Armee der Nazis postiert und auch diese Truppen wollte man von der Verteidigung der Normandie abhalten. Um die Pläne glaubhaft zu machen und die Deutschen davon Notiz nehmen zu lassen, schickten die Funker fingierte Botschaften hin und her in denen sie von den Plänen berichteten und gleichzeitig Fehler einbauten, die es den Deutschen ermöglichten die Nachrichten schneller zu entschlüsseln. Um die deutschen Militärs endgültig zu überzeugen, stellten die Briten Attrappen von Kriegsschiffen und Kampfflugzeugen auf. Die Maßnahmen gingen auf. Die Deutschen konzentrierten sich auf Kampfhandlungen in Norwegen und Calais und die Landung der Alliierten in der Normandie glückte.[235]

8. Die Nachkriegszeit

8.1. Der kalte Krieg

Nachdem der Zweite Weltkrieg beendet war, zerbrach die Allianz an der Kontroverse über die Folgen des Krieges. In der Konferenz von Jalta wurde festgelegt, dass die Länder, die von den Nazis eingenommen worden waren, befreit werden sollten, doch nur ein Jahr später waren die osteuropäischen Länder von der Sowjetunion besetzt worden. Der eiserne Vorhang fiel. Die Zeit des kalten Krieges war insbesondere durch Spionage aller Art, z.B. militärische, politische, wirtschaftliche,…, geprägt. Die Sowjetunion war während des Zweiten Weltkriegs eine alliierte Macht gewesen. Nachrichten wurden zwar abgefangen, die Dechiffrierung blieb aber aus, weil die Nachrichten der Nazis wichtiger gewesen waren. Das wurde nun nachgeholt, allerdings mit mäßigem Erfolg, da die Russen zu dieser Zeit bereits One-Time-Pads

[235] Wrixon, Fred: Geheimsprachen, S. 104 ff.
http://de.wikipedia.org/wiki/Operation_Fortitude, letzter Zugriff: 25.03.2009.

verwendeten. Einige Erfolge konnten die amerikanischen Kryptoanalytiker dennoch verbuchen, da die sowjetischen Funker bei der Verwendung der One-Time-Pads nicht immer die notwendige Vorsicht walten ließen und sich wiederholende Ziffernfolgen in Schlüsseln generierten. Informationstechnisch waren Informationen der Spione allerdings oftmals wichtiger.[236]

8.2. Die NSA

Mit der schockierenden Erkenntnis, dass es der Sowjetunion 1949, mit Hilfe von Spionen, gelungen war die Atombombe nachzubauen, führten die USA die „Armed Forces Security Agency“ ein, die im Koreakrieg einige Pannen verursachten. Daher wurden sie 1952 von der „National Security Agency“ (kurz: NSA) abgelöst. Die NSA ist noch heute aktiv, sie ist der zentrale Nachrichtendienst der USA und untersteht dem Verteidigungsministerium. Wegen ihrer umfassenden, weltumspannenden Aufklärung gerät sie immer wieder in die Kritik von Datenschützern. Mit Echelon hält die NSA beispielsweise ein System bereit, dass den weltweiten Funkverkehr aufzeichnen kann. Tatsächlich stammt Echelon aus der Zeit des Kalten Krieges und wurde dazu verwendet die Sowjetunion abzuhören. Seit Ende des Kalten Krieges wurden aber immer wieder Fälle bekannt in denen Echelon zur Industriespionage missbraucht wurde, um die amerikanische Wirtschaft anzukurbeln. Die massive Informationsflut von Echelon veranlasste die Agenten der NSA dazu neue Programme und Verfahren zu konzipieren, um die Nachrichten auf Schlagwörter zu durchsuchen, welche die wichtigen Nachrichten von den Unwichtigen trennen und die Aufklärungsarbeit effektiver machen.[237]

8.3. Die Juwelen

Jewels (Deutsch: Juwelen) war der Codename für die Chiffriermaschinen, welche die Diplomaten der USA in Moskau für die Korrespondenz mit der CIA und NSA verwendeten. Die Juwelen unterlagen strengster Geheimhaltung und waren in speziell abgesicherten Räumen untergebracht. Trotz massiver Sicherheitsvorkehrungen war es dem KGB gelungen, die Leitung, über die Jewels-

[236] Wrixon, Fred: Geheimsprachen, S. 110 ff.
[237] Wrixon, Fred: Geheimsprachen, S. 116 ff.
http://de.wikipedia.org/wiki/National_Security_Agency, letzter Zugriff: 26.03.2009.

Signale gesendet wurden, anzuzapfen und so die Nachrichten abzuhören. Außerdem hatten sie die Drucker der Maschinen so manipuliert, dass sie den Text noch vor seiner Verschlüsselung abfangen konnten. Den Klartext verglichen sie mit dem chiffrierten Text um Jewels zu knacken, mit schlimmen Folgen für die USA: Viele ihrer Undercover-Agenten sowie Spione und Informanten wurden enttarnt und Arbeitsmethoden der NSA aufgedeckt. Verantwortlich für die erfolgreichen Angriffe auf Jewels waren wieder einmal Spione, diesmal aus den eigenen Reihen der amerikanischen Geheimdienste.[238]

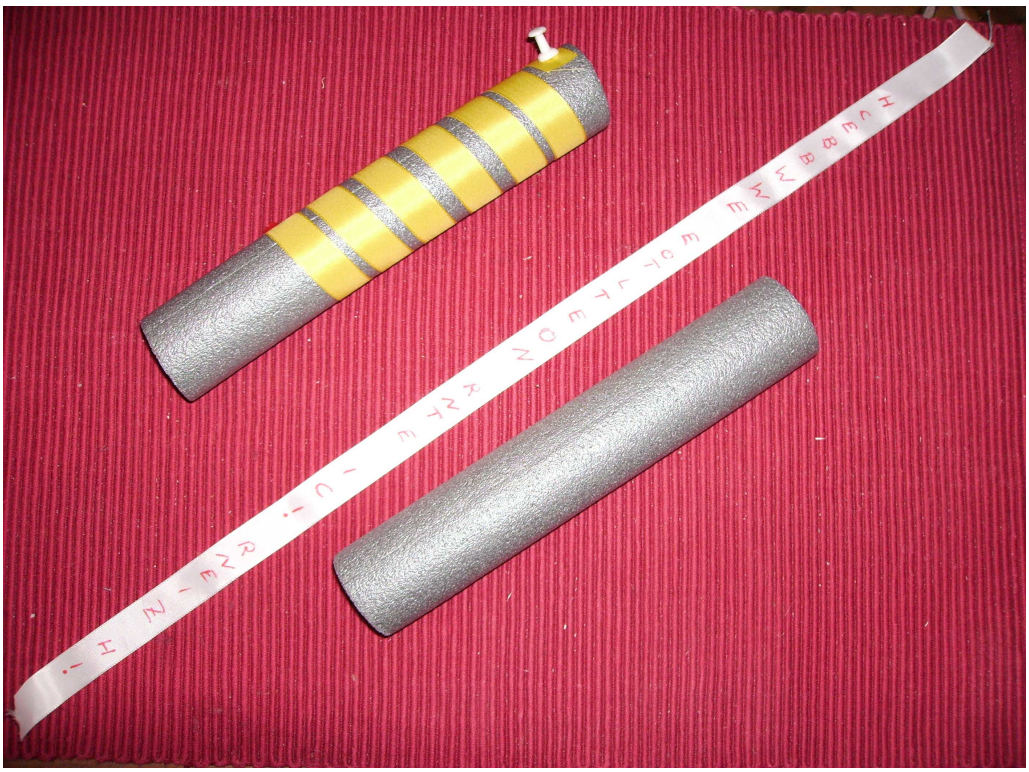
[238] Wrixon, Fred: Geheimsprachen, S. 121 ff.

II. Verlaufspläne und Materialien zu den Unterrichtsstunden

1. Skytale von Sparta

Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen die Wichtigkeit von Geheimnissen, Einsatzmöglichkeiten der Verschlüsselung und die Skytale von Sparta.
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS erkennen, dass jeder Mensch Geheimnisse hat, die er schützen will.
Fach:	Mathematik	- Die SuS wissen, dass Geheimschriften eine Möglichkeit bieten geheime Nachrichten zu übermitteln.
Datum:		- Die SuS wissen, dass Geheimschriften keine Erfindung der Neuzeit sind.
Thema der Stunde		- Die SuS kennen die Begriffe verschlüsseln, entschlüsseln und Schlüssel (Code).
Geheimschriften, Skytale(Einführungsstunde)		- Die SuS kennen die Methode der Skytale von Sparta und können mit ihr Texte ver- und entschlüsseln.
		- Die SuS kennen das Problem des Schlüsselaustauschs bei der Skytale.

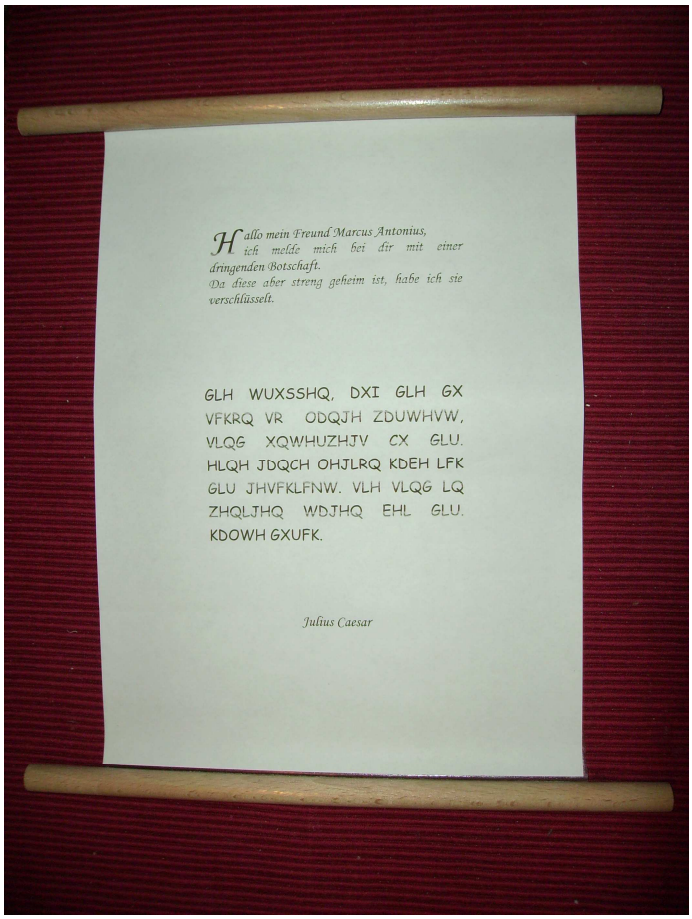
Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und bittet die Schüler in den Sitzkreis.	SuS kommen mit ihren Stühlen in den Sitzkreis.	-	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Einstieg	Der Lehrer zeigt den Schülern eine Schatzkiste mit einer Schriftrolle auf der eine geheime Nachricht steht, die es zu entschlüsseln gilt. Dann fragt er die Schüler, ob sie Geheimnisse haben (Tagebücher, ...) und wie sie diese schützen.	Die Schüler versuchen die geheime Botschaft mit Hilfe der Skytale zu entschlüsseln. Im anschließenden Gespräch teilen sie ihre Erfahrungen mit und bringen sich damit in die Diskussion ein.	Schatzkiste, geheime Botschaft, Skytale	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Erarbeitungsphase	Gemeinsam wird geklärt wie lange es schon Geheimschriften gibt. Außerdem werden die Begriffe verschlüsseln, entschlüsseln und Schlüssel erarbeitet und das Verfahren mittels der Skytale eingehender betrachtet.	Die Schüler bringen sich wiederum mit ihren Erfahrungen und ihrem bisherigen Wissen ein, außerdem arbeiten sie mit den Skytalen	Kleine Kiste, Skytale	Frontalunterricht, Unterrichtsgespräch
15 Minuten	Übungsphase	Der Lehrer steht den Schülern mit Rat und Tat zur Seite.	Die Schüler arbeiten mit gleichen Skytalen. Sie ver- und entschlüsseln dabei geheime Botschaften.	Geheime Botschaften, Skytale, Papierstreifen.	Partnerarbeit
5 Minuten	Abschluss	Der Lehrer fragt die Schüler nach Problemen des Verfahrens und verarbschiedet sie anschließend.	Die Schüler beratschlagen über Probleme, packen ihre geheimen Botschaften und Skytalen weg und verabschieden den Lehrer.	-	Frontalunterricht, Unterrichtsgespräch

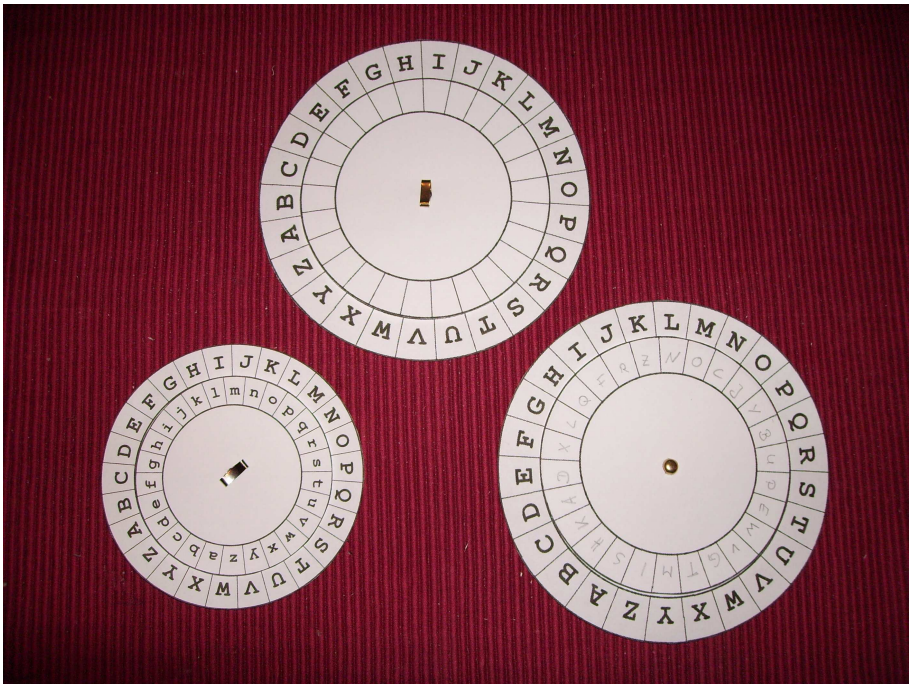


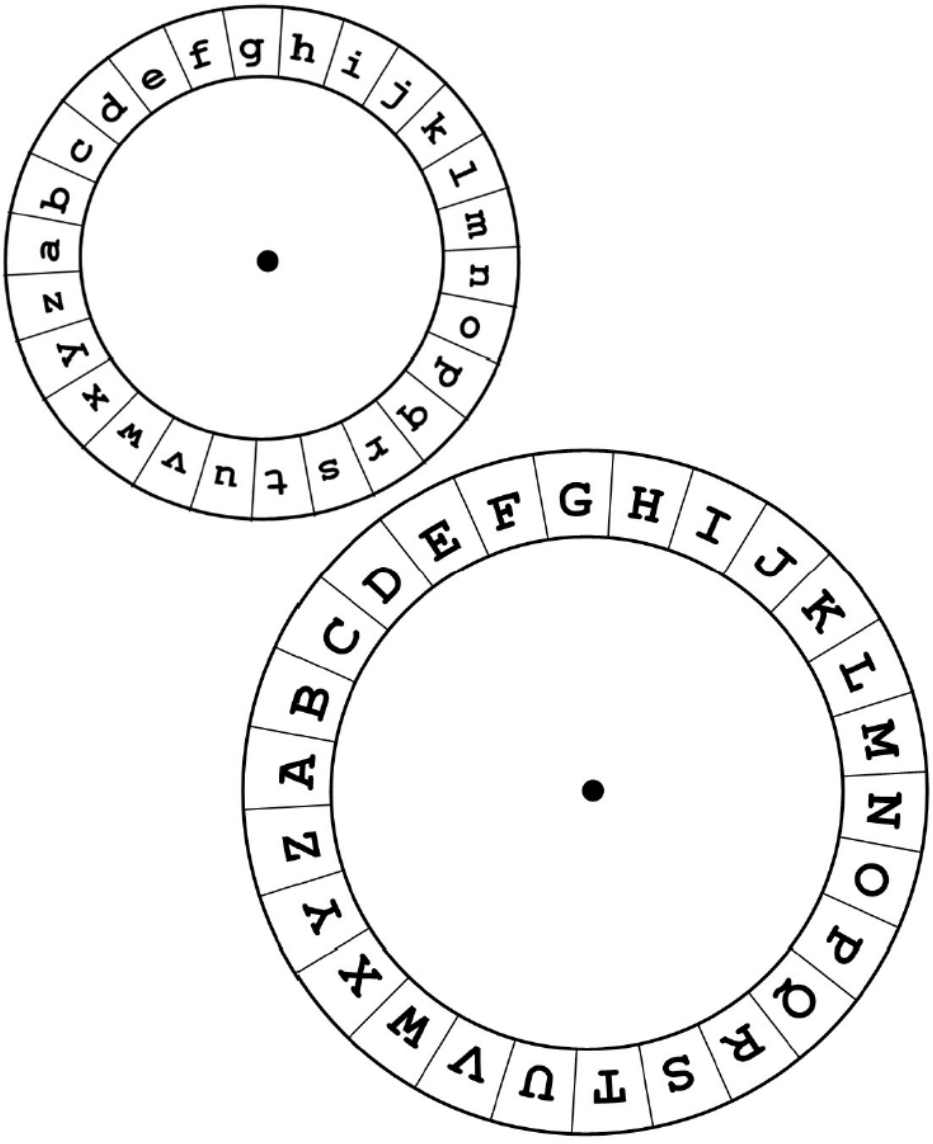
2. Caesar-Verfahren

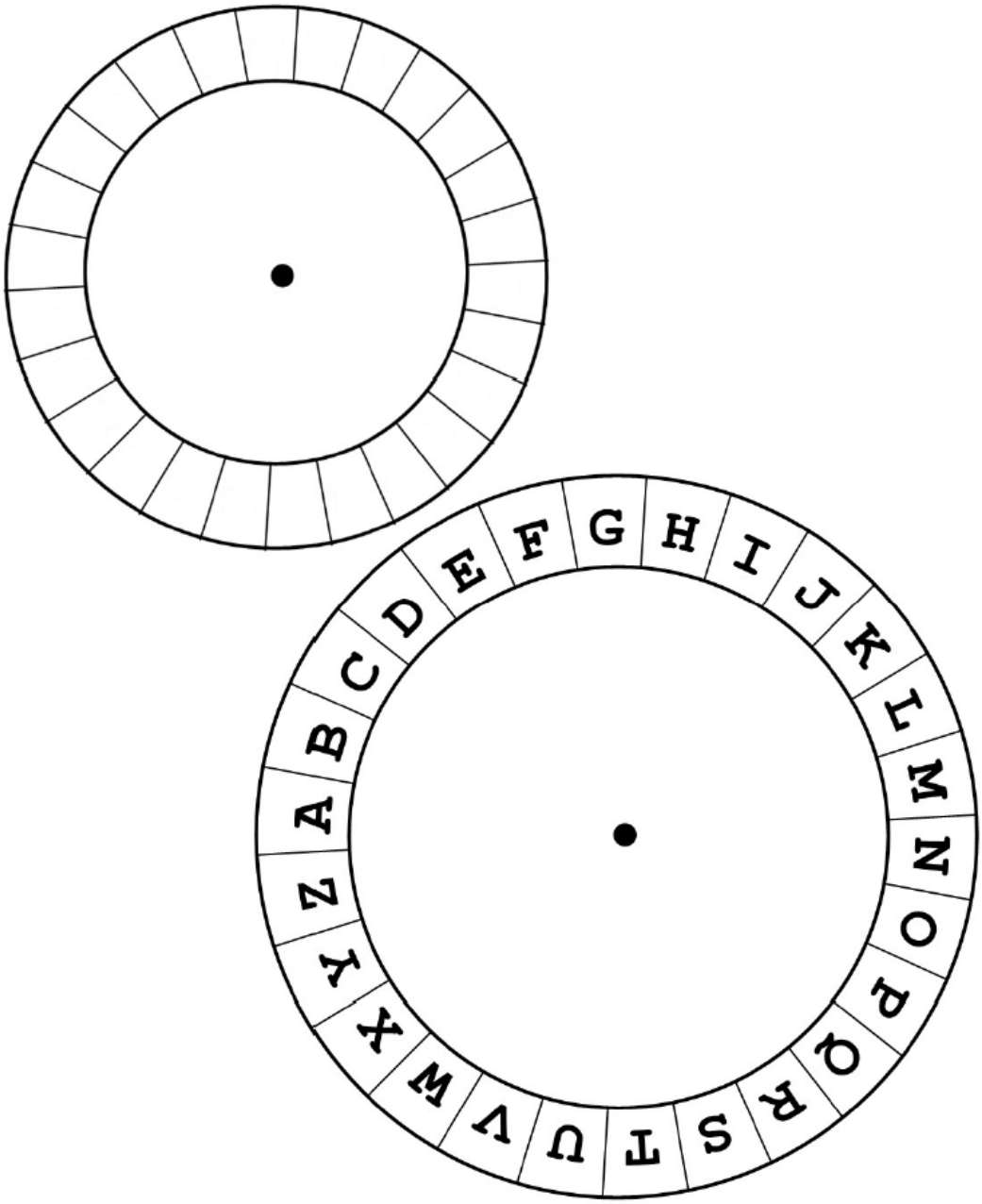
Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen das Verfahren zur Verschlüsselung von Caesar und können es anwenden.
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS können die Verfahren von Caesar und der Skytale vergleichen.
Fach:	Mathematik	- Die SuS wissen, dass es andere Möglichkeiten zur Verschlüsselung gibt als nur die Umstellung der Buchstaben.
Datum:		- Die SuS erkennen die Möglichkeit Buchstaben zu ersetzen.
Thema der Stunde		- Die SuS kennen das Caesar-Verfahren und können es anwenden.
Geheimschriften, Caesar-Verfahren		- Die SuS erkennen Probleme des Caesar-Verfahrens (Schlüsselaustausch, Buchstabenhäufigkeit)

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und bittet die Schüler in den Sitzkreis.	SuS kommen mit ihren Stühlen in den Sitzkreis.	-	Frontalunterricht, Unterrichtsgespräch
5 Minuten	Einstieg	Der Lehrer zeigt den Schülern erneut die Schatzkiste mit einer neuen geheimen Botschaft, die es zu entschlüsseln gilt.	Die Schüler versuchen die geheime Botschaft mit Hilfe des Caesar-Verfahrens zu entschlüsseln.	Schatzkiste, geheime Botschaft	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Erarbeitungsphase	Gemeinsam wird das Caesar-Verfahren im Sitzkreis erarbeitet. Dabei werden unterschiedliche Varianten von dem typischen Caesar-Verfahren (Verschiebung um 3 Stellen) bis zur Caesar-Scheibe erörtert.	Die Schüler bringen sich mit ihren Ideen in die Diskussion ein.	Caesar-Scheibe	Frontalunterricht, Unterrichtsgespräch
20 Minuten	Übungsphase	Der Lehrer steht den Schülern mit Rat und Tat zur Seite.	Die Schüler basteln sich eigene Caesar-Scheiben. Schnelle Schüler können diese dann bereits zum ver- und entschlüsseln geheimer Nachrichten verwenden.	Caesar-Scheibe, geheime Botschaften	Einzelarbeit (schnelle Schüler können in Partnerarbeit Texte verschlüsseln)
5 Minuten	Abschluss	Der Lehrer fragt die Schüler nach Problemen bei diesem Verfahren. Anschließend verarbschiedet er sie.	Die Schüler diskutieren Probleme, packen ihre Caesar-Scheiben weg und verabschieden den Lehrer.	-	Frontalunterricht, Unterrichtsgespräch








A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

3. Vigenère-Verfahren

Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen das Vigenère-Verfahren und können es anwenden.
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS kennen die Problematik des Caesar-Verfahrens (Buchstabenhäufigkeit).
Fach:	Mathematik	- Die SuS kennen das Verfahren von Vigenère und können es anwenden.
Datum:		- Die SuS vergleichen das Caesar- und das Vigenère-Verfahren.
Thema der Stunde		- Die SuS erkennen den Vorteil des Vigenère-Verfahrens gegenüber dem Caesar-Verfahren.
Geheimschriften, Vigenère-Verfahren		- Die SuS erkennen Probleme des Vigenère-Verfahrens (Schlüsselwort, Schlüsselaustausch)

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und begrüßt die Schüler.	Die Schüler begrüßen den Lehrer.	-	Frontalunterricht
5 Minuten	Einstieg	Der Lehrer zeigt den Schülern einen Text, der mit Hilfe des Caesar-Verfahrens verschlüsselt wurde, für den allerdings kein Code vorliegt.	Die Schüler überlegen, wie man den Code dennoch herausfinden könnte.	Geheimer Text	Frontalunterricht, Unterrichtsgespräch
5 Minuten	Erarbeitungsphase I	Der Lehrer stellt die Problematik einer unterschiedlichen Buchstabenhäufigkeit vor.	Die Schüler überlegen welche Probleme dieser Umstand für das Caesar-Verfahren bringt.	Tabelle Buchstabenhäufigkeit	Frontalunterricht, Unterrichtsgespräch
5 Minuten	Übungsphase I	Der Lehrer gibt den Schülern den Auftrag die Buchstaben zu zählen und mit der typischen Buchstabenhäufigkeit zu vergleichen.	Die Schüler zählen die Buchstaben und vergleichen die Häufigkeit mit der Tabelle.	Geheimer Text, Tabelle Buchstabenhäufigkeit	Einzelarbeit

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
10 Minuten	Erarbeitungsphase II	Aus der Analyse des Textes ergibt sich die Notwendigkeit z.B. den Buchstaben e mit mehreren verschiedenen Buchstaben zu verschlüsseln (polyalphabetische Verschlüsselung). Der Lehrer stellt die Vigenère-Tafel vor und fragt die Schüler, wie man damit einen Text verschlüsseln könnte.	Die Schüler teilen ihre Ideen mit	Vigenère-Tafel	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Übungsphase II	Der Lehrer steht den Schülern mit Rat und Tat zur Seite.	Die Schüler arbeiten in Partnerarbeit mit der Vigenère-Tafel.	Vigenère-Tafeln	Partnerarbeit
5 Minuten	Abschluss	Der Lehrer fragt die Schüler nach Problemen bei diesem Verfahren. Anschließend verarbschiedet er sie.	Die Schüler überlegen sich Probleme des Verfahrens und verabschieden den Lehrer.	-	Frontalunterricht, Unterrichtsgespräch

Aufgabe (zum Einstieg):

Zähle die Buchstaben und versuche herauszufinden wie der folgende Satz wirklich lautet.

Verwende dazu die Tabelle unten.

Dfc zndfcdp Usdepdn.

Lösung: _____

Geheimbuchstabe	Wie oft kommt der Buchstabe vor?	Echter Buchstabe
D		
C		
F		
P		
N		
U		
S		
E		
Z		

Die Häufigkeit der Buchstaben in der deutschen Sprache.

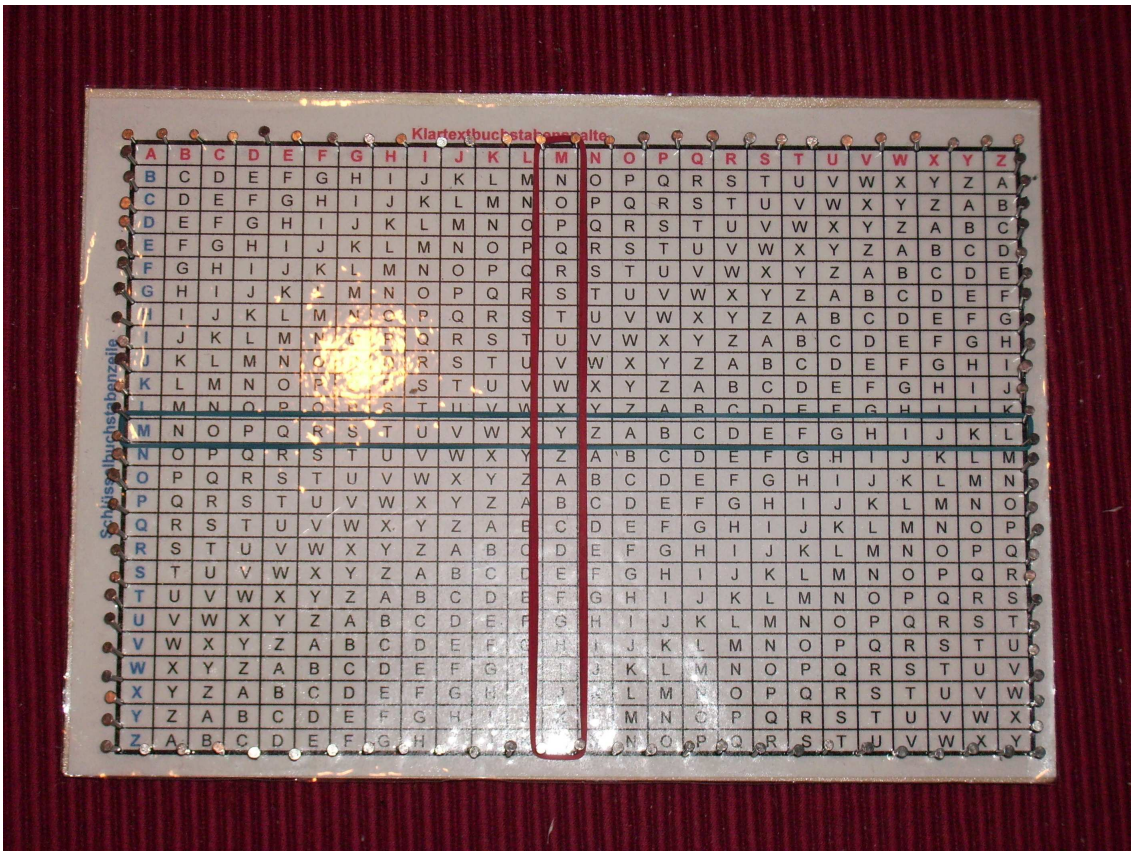
Platz	Buchstabe	Anzahl je 100
1	E	17,40
2	N	9,78
3	I	7,55
4	S	7,27
5	R	7,00
6	A	6,51
7	T	6,15
8	D	5,08
9	H	4,76
10	U	4,35
11	L	3,44
12	C	3,06
13	G	3,01
14	M	2,53
15	O	2,51
16	B	1,89
17	W	1,89
18	F	1,66
19	K	1,21
20	Z	1,13
21	P	0,79
22	V	0,67
23	J	0,27
24	Y	0,04
25	X	0,03
26	Q	0,02

Aufgabe in Übungsphase I:

Schlüsselwort: Blume

TELQRH RYTIJXY NSUDWTEGE!

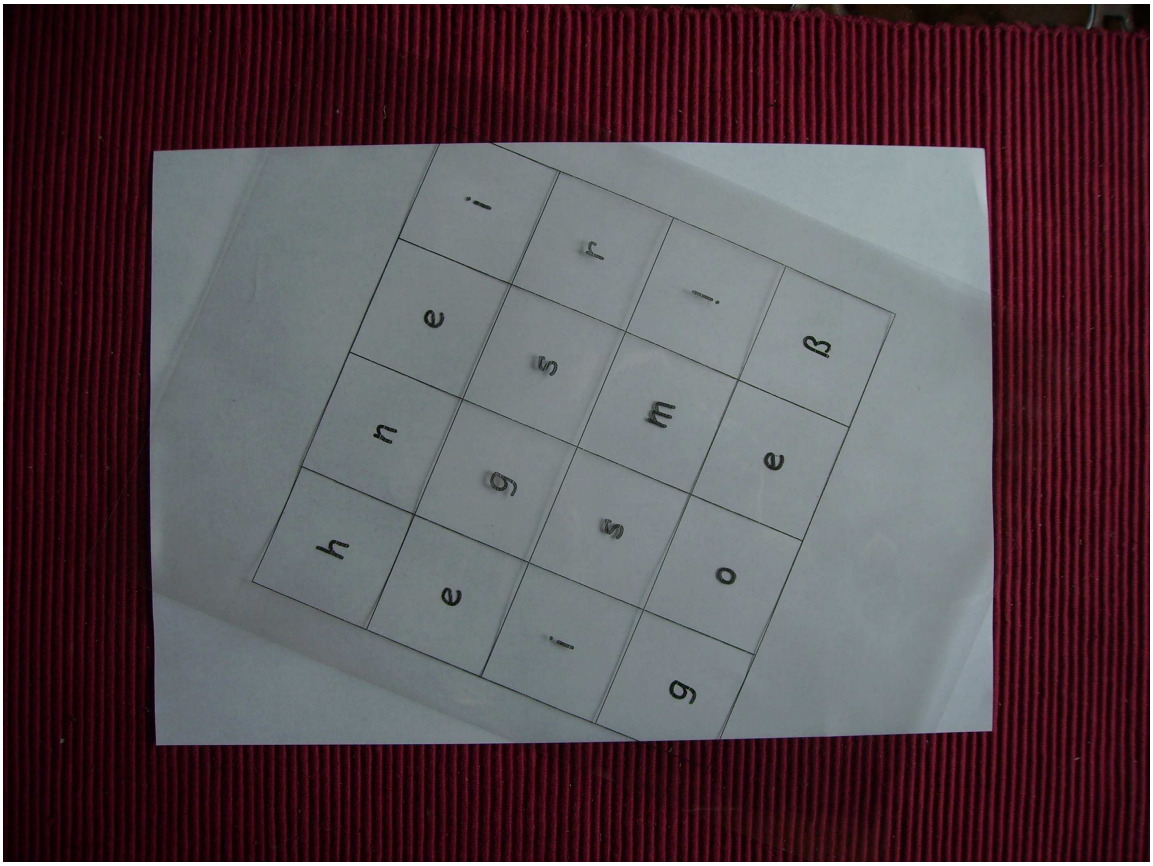
Klartext: _____

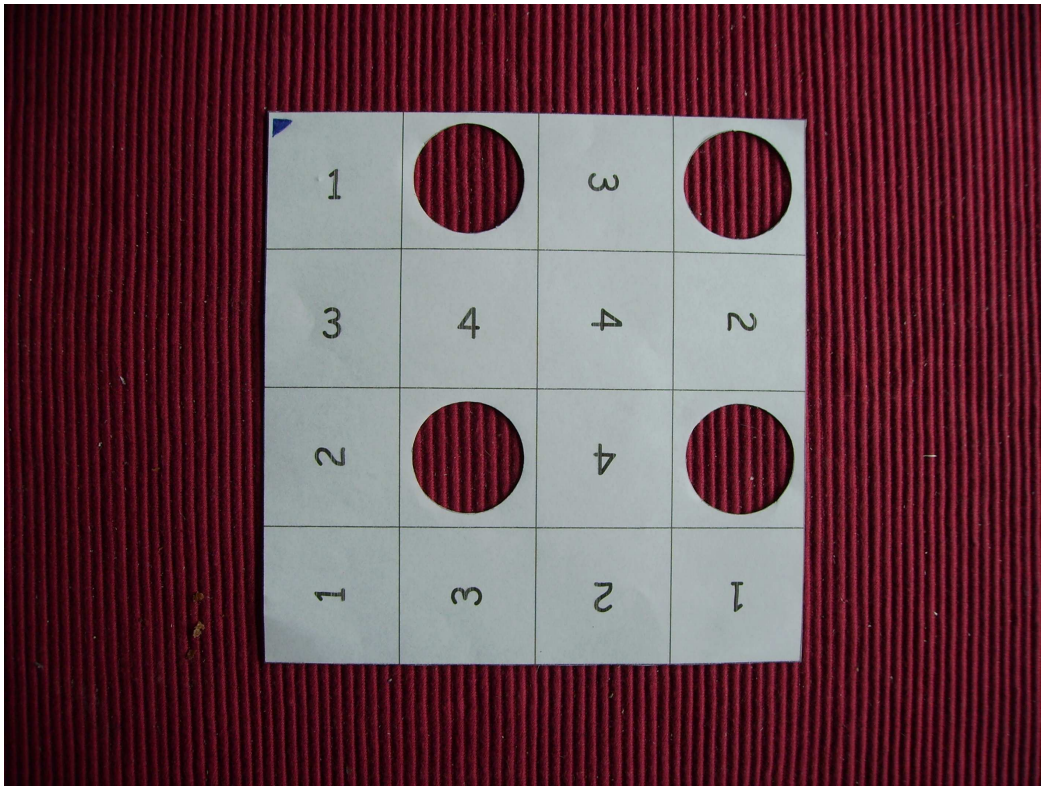


4. Fleissner-Methode

Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen die Fleissner-Verschlüsselung und können damit arbeiten.
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS kennen das Verschlüsselungsverfahren mit Hilfe der Fleissner-Schablone
Fach:	Mathematik	- Die SuS kennen die Gemeinsamkeiten von Schablone und Skytale (Zeichenverschiebung, Transposition)
Datum:	03.03.2009	-Die SuS erkennen die Methode die hinter der Schablonenverschlüsselung steckt
Thema der Stunde		- Die SuS können mit der Schablone ver- und entschlüsseln
Fleissner-Schablone		- Die SuS können eine eigene Schablone herstellen.
		- Die SuS kennen Probleme des Verfahrens mit der Fleissner-Schablone

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und begrüßt die Schüler.	Die SuS begrüßen den Lehrer und kommen zur Ruhe.	-	Frontalunterricht
5 Minuten	Einstieg	Der Lehrer legt eine Folie mit einer verschlüsselten Nachricht auf den OHP.	Die SuS betrachten den verschlüsselten Text und entwickeln Ideen wie dieser verschlüsselt sein könnte. Außerdem probieren sie ihn zu entschlüsseln.	OHP, Folie	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Erarbeitungsphase	Der Lehrer zeigt den Schülern die passende Schablone. Gemeinsam wird die Funktionsweise der Schablone besprochen.	Die SuS überlegen, wie sich die Schablone dazu eignet den Text zu entschlüsseln. Schüler mit Ideen kommen nach vorne und erproben diese.	OHP, Folie, Schablone	Frontalunterricht, Unterrichtsgespräch
20 Minuten	Übungsphase	Der Lehrer achtet darauf, dass die SuS keinen Unsinn mit Hammer und Henkellocheisen machen.	Die SuS erstellen sich eigene Schablonen. Auftretende Probleme werden im Klassenverband angesprochen und erörtert. Schnelle Schüler können anschließend Nachrichten verschlüsseln.	Henkellocheisen, Hammer, Schablonenvordrucke, Platten	Einzelarbeit, Unterrichtsgespräch
5 Minuten	Abschluss	Der Lehrer fragt die Schüler nach Problemen des Verfahrens und verarbschiedet sie anschließend.	Die Schüler beratschlagen über Probleme, packen Botschaften und Schablonen weg und verabschieden den Lehrer.	-	Frontalunterricht, Unterrichtsgespräch




1 3
3 4 4 2
2 4
1 3 2 1


1 2 3
1 2 4 3
3 4 4 2
2 3
1

5. Schlüsselaustausch

Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen das Problem der Schlüsselübergabe und eine Lösung dafür.
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS kennen die Wichtigkeit des Schlüssels bei den klassischen Verschlüsselungsalgorithmen.
Fach:	Mathematik	- Die SuS kennen Die Problematik eines ungesicherten Schlüsselaustauschs.
Datum:		- Die SuS erkennen Die Problematik einer Endlosreihe beim verschlüsseln des Schlüssels.
Thema der Stunde		- Die SuS kennen das Prinzip der Einwegfunktion.
Schlüsselübertragung		- Die SuS kennen eine mögliche Lösung für das Problem der Schlüsselübergabe.

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und begrüßt die Schüler.	Die SuS kommen zur Ruhe und begrüßen den Lehrer.	-	Frontalunterricht
5 Minuten	Einstieg	Der Lehrer liest den Schülern eine Geschichte vor, die sich mit dem Problem der Schlüsselübergabe beschäftigt.	Die Schüler lauschen der Geschichte.	Geschichte	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Erarbeitungsphase	Lehrer und Schüler erarbeiten im Unterrichtsgespräch gemeinsam, wie man das Problem der Schlüsselübergabe mit Hilfe von Einwegfunktionen lösen könnte. Dabei werden die nötigen Begriffe erklärt. Das Problem wird anhand einer Analogie mit Farben gelöst.		Farben	Frontalunterricht, Unterrichtsgespräch
20 Minuten	Übungsphase	Der Lehrer gibt den Schülern Hilfestellungen.	Die SuS erarbeiten sich im Partnerarbeit Schlüssel ohne sie zu übergeben.	Farben	Partnerarbeit
5 Minuten	Abschluss	Der Lehrer verarbschiedet die Schüler.	Die Schüler verabschieden den Lehrer.	-	Frontalunterricht

Einstiegsgeschichte:

Was für ein Mist. Ausgerechnet diesen Sommer musste Peter Shaw mit seinen Eltern in den Urlaub fahren. Dabei hätte es so ein aufregender Sommer für die drei Fragezeichen werden können. Nun aber waren sie getrennt voneinander, doch sie hatten sich versprochen, jede Woche einen Brief zu schreiben, um in Kontakt zu bleiben.

Justus Jonas und Bob Andrews saßen in ihrem Detektivbüro und hatten den ersten Brief fertig geschrieben. Justus wollte den Brief gerade zukleben, als Bob ihn aufhielt:

„Warte," rief er, „was, wenn der Brief falsch zugestellt wird und ihn jemand öffnet. Niemand soll erfahren, was darin steht, außer Peter."

„Du hast recht." antwortete Justus. Zum Glück hatten sie vor einigen Monaten gelernt, wie man einen Text so verschlüsselt, dass ihn niemand mehr lesen kann. Also verschlüsselten sie ihre Nachricht an Peter.

„Und was machen wir jetzt mit dem Schlüssel?“ fragte Justus. „Wir können ihn nicht einfach so zu der Nachricht in den Umschlag legen.“

„Wir müssen ihn ebenfalls verschlüsseln“ antwortete Bob „aber dann haben wir wieder einen neuen Schlüssel und auch den müssten wir dann verschlüsseln. Das geht immer so weiter. Wann hören wir damit auf?“

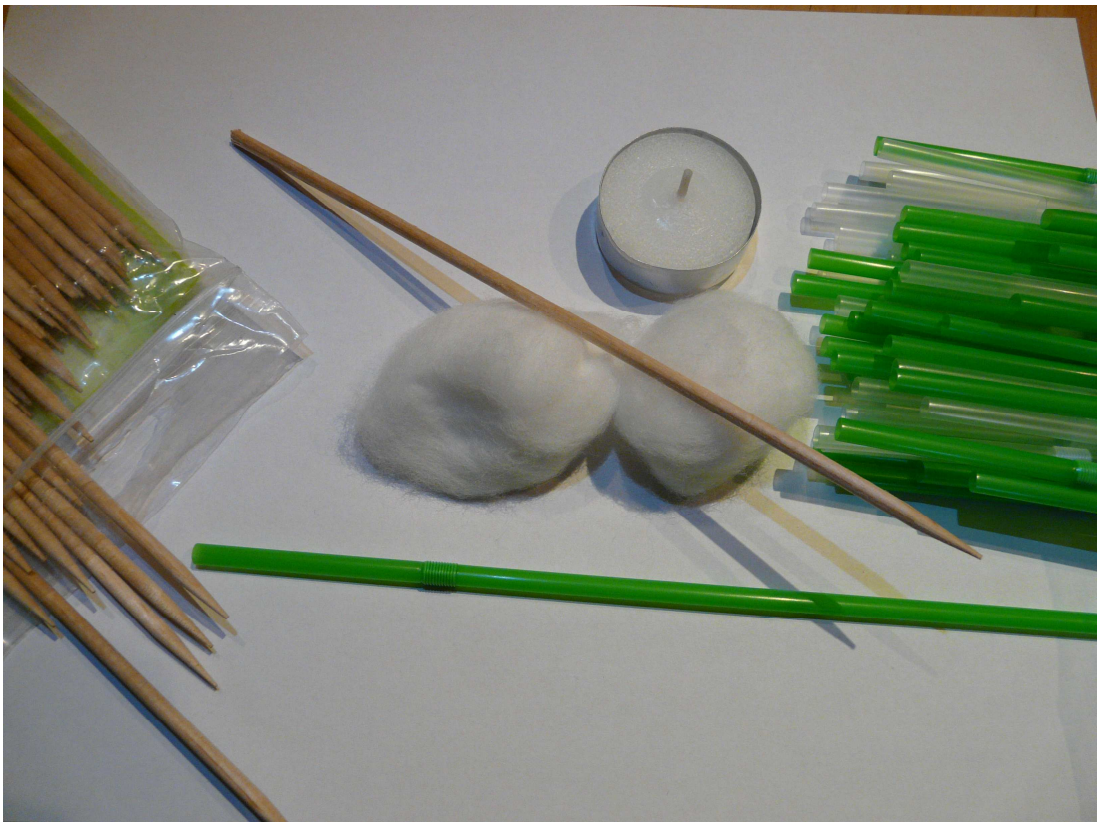
Habt ihr eine Idee, wie man das Problem der Schlüsselübergabe lösen könnte?

6. Steganografische Methoden

Name:	Sebastian Connette	Ziele der Stunde
Dozent:	Ziegenbalg, Borys	Die SuS kennen Möglichkeiten der Steganografie
Mentor:	Frau Blume	
Schule:	Anne-Frank-GHS	Feinziele der Stunde
Klasse:	4d	- Die SuS wissen, das Botschaften nicht nur verschlüsselt, sondern auch versteckt werden.
Fach:	Mathematik	- Die SuS kennen den Unterschied zwischen Verschlüsselung und Verstecken einer Botschaft
Datum:		- Die SuS kennen klassische steganografische Methoden (Tätowierung, Mikrofilm, Mikropunkt, Musik)
Thema der Stunde		- Die SuS kennen die Methode markierter Buchstaben im Text
Steganografie		- Die SuS kennen Geheimtinten und können einen Geheimschreiber selbst herstellen.
		- Die SuS kennen Möglichkeiten digitaler Steganografie (computerbasiert, digitale Wasserzeichen, ...)

Zeit	Phase	Lehrertätigkeit	Schülertätigkeit	Medien	Sozialform
5 Minuten	Begrüßung	Der Lehrer beginnt die Stunde und begrüßt die Schüler.	Die SuS begrüßen den Lehrer und kommen zur Ruhe.	-	Frontalunterricht
5 Minuten	Einstieg	Der Lehrer zeigt den Schülern ein weißes Blatt Papier. Er leuchtet mit blauem Licht darauf und eine Schrift wird sichtbar.	Die SuS betrachten das weiße Blatt Papier, bzw. die geheime Nachricht.	Papier, Botschaft, Geheimstift	Frontalunterricht, Unterrichtsgespräch
10 Minuten	Erarbeitungsphase	Der Lehrer fragt die Schüler nach den Unterschieden zu den bereits bekannten Verfahren. Anschließend erzählt er den Schülern von klassischen steganografischen Methoden.	Die SuS teilen ihre Ideen und Erfahrungen mit und hören dem Lehrer zu.	-	Frontalunterricht, Unterrichtsgespräch
20 Minuten	Übungsphase	Der Lehrer hilft den Schülern bei Fragen und Problemen.	Die SuS basteln sich mit den zur Verfügung gestellten Materialien eigene Geheimstifte und schreiben sich gegenseitig geheime Nachrichten.	Strohhalme, Watte, Zitronen, Milch, Kerzen	Einzelarbeit, Partnerarbeit, Gruppenarbeit
5 Minuten	Abschluss	Der Lehrer verabschiedet die Schüler	Die SuS verabschieden den Lehrer	-	Frontalunterricht, Unterrichtsgespräch


GEHEIM



Die Seiten 44 - 58 des Anhangs der Originalarbeit (Unterrichts-Dokumentationen) wurden aus datenschutzrechtlichen Gründen entfernt.