Einführung

In diesem Tutorial wird erklärt, wie Sie den Bombe-Simulator sowie den Checking Machine Simulator für jede mit Enigma verschlüsselte Nachricht (und Crib; mehr dazu später) verwenden können. Es wird nicht im Detail erklärt, warum die Bombe funktioniert oder wie sie aufgebaut ist. Der Bombe-Simulator soll so genau wie möglich sein, aber es kann Unterschiede zur Funktionsweise einer echten Bombe geben. Die Autoren stehen in keiner Verbindung zu Bletchley Park, was die Turing-Bombe betrifft, aber wir empfehlen allen, die sich für diese Dinge interessieren, das National Museum of Computing (TNMOC) zu besuchen, das sich in Bletchley Park, aber außerhalb des Hauptmuseums von Bletchley Park befindet, um eine voll funktionsfähige Bombe-Nachbildung in Aktion zu sehen.

Ein paar Worte zur Enigma-Maschine und zur Bombe

Es wird vorausgesetzt, dass der Leser über Grundkenntnisse der Funktionsweise der Enigma-Maschine verfügt. Dennoch wird hier ein kurzer Überblick gegeben, um einige der Begriffe zu erklären, die bei der Arbeit mit der Bombe verwendet werden.

Die Enigma-Maschine funktioniert, indem sie einen Stromkreis mit einem über die Tastatur eingegebenen Buchstaben, mehreren Verschlüsselungsstufen und einer Lampe, die den verschlüsselten Buchstaben anzeigt, erstellt. In jeder Verschlüsselungsstufe wird der eingegebene Buchstabe durch einen anderen Buchstaben ersetzt, der an die nächste Stufe weitergeleitet wird. Die Stufen sind:

- Die Stecktafel. Die Stecktafel bietet die Möglichkeit, bis zu zehn Buchstabenpaare auszutauschen, indem Kabel zwischen den Buchstaben verbunden werden. Wenn beispielsweise ein Kabel zwischen A und E verbunden ist, wird durch Drücken von A auf der Tastatur tatsächlich ein E an die nächste Stufe gesendet.
- Die Rotoren. Die gängigsten Enigma-Maschinen haben drei Rotorschlitze mit acht Rotormodellen mit unterschiedlicher interner Verdrahtung zur Auswahl. Die Rotoren sind mit römischen Ziffern gekennzeichnet: I bis VIII. Jeder Rotor hat einen Ring, auf dem das Alphabet aufgedruckt ist. Der Rotor kann so gedreht werden, dass ein bestimmter Buchstabe in einem Fenster auf der Enigma zu sehen ist. Dies wird als Position des Rotors bezeichnet. Der Ring kann in Bezug auf den Rotor gedreht werden, dies wird als Ringeinstellung bezeichnet. Weitere Einzelheiten finden Sie im entsprechenden Kapitel weiter unten.
- Der Reflektor. Nach dem Passieren des Reflektors durchläuft das Signal erneut die Rotoren und die Stecktafel, jedoch in umgekehrter Reihenfolge. Es gibt drei verschiedene, häufig verwendete Reflektormodelle, die mit A, B und C gekennzeichnet sind.

Um eine Nachricht zu verschlüsseln oder zu entschlüsseln, musste ein Enigma-Maschinenbediener eine Reihe von Einstellungen an der Maschine vornehmen. Diese bilden zusammen den Schlüssel für die Nachricht.
Die verschiedenen Teile des Schlüssels sind die folgenden:

- Welche Rotoren werden verwendet und in welcher Reihenfolge werden sie in die Enigma eingesetzt?
- Die Ausgangsposition der Rotoren. Wenn die Ausgangsposition beispielsweise „HEJ" lautet, wird der linke Rotor auf H, der mittlere auf E und der rechte auf J gedreht.
- Die Ringstellung der Rotoren. Diese wird genauso wie die Startposition geschrieben: ein Buchstabe für jeden Rotor.
- Die Stecktafelverbindungen. Diese werden als eine Folge von 10 Buchstabenpaaren geschrieben.

Angenommen, wir verwenden eine Enigma mit drei Rotoren und acht verfügbaren Rotoren zur Auswahl und müssen zehn Kabel verwenden, um zwanzig Buchstaben auf der Stecktafel miteinander zu verbinden, dann sieht der Schlüsselraum wie folgt aus:

Anzahl der möglichen Auswahlmöglichkeiten für Rotoren und
Rotorreihenfolge: 336 Anzahl der möglichen Ringeinstellungen: 17.576
Anzahl der möglichen Startpositionen der Rotoren: 17.576
Anzahl der Möglichkeiten, 10 Kabel im Steckbrett zu verbinden: 150.738.274.937.250

Es ist offensichtlich, dass der Steckbrett bei weitem den größten Beitrag zum

Schlüsselraum leistet.

Der Zweck der Bombe-Maschine besteht darin, bei der Suche nach dem für eine bestimmte Nachricht verwendeten Schlüssel zu helfen, insbesondere bei den Einstellungen der Stecktafel. Die Maschine kann als eine Reihe vereinfachter Enigma-Maschinen betrachtet werden, die so miteinander verbunden sind, dass sie viele unmögliche Stecktafeleinstellungen ausschließen und dem Benutzer die verbleibenden, potenziell richtigen Einstellungen zur weiteren Analyse zur Verfügung stellen können. Die Bombe kann alle 17.576 Startpositionen der Rotoren durchsuchen, aber die Reihenfolge und die Typen der Rotoren müssen manuell getestet werden.

Weitere Details zu Rotoren und Trommeln

Bei jedem Tastendruck auf der Enigma bewegt sich der rechte Rotor um einen Schritt. Wenn er eine bestimmte Position erreicht, löst er eine Bewegung des mittleren Rotors um einen Schritt aus. Dies wird als Umkehrung bezeichnet. Auf die gleiche Weise bewegt der mittlere Rotor den linken Rotor. Ein Metallstück, das als „Kerbe” bezeichnet wird, löst den Mechanismus aus, der den nächsten Rotor aktiviert. Normalerweise gibt es nur eine Kerbe pro Rotor, sodass pro Umdrehung ein Umschlag ausgelöst wird, aber einige Rotoren haben zwei Kerben.

Die Ringeinstellung an den Enigma-Rotoren ändert nichts an der tatsächlichen Verschlüsselung, die von diesem Rotor durchgeführt wird. Die Verdrahtung im Inneren eines Rotors ist für diesen bestimmten Rotor immer gleich. Die Ringeinstellung ändert nur die Position, an der der Rotor einen Buchstaben in einen anderen verschlüsselt.
Das bedeutet, dass ein Rotor, dessen Ring auf A eingestellt ist, in Position A dem gleichen Rotor entspricht, dessen Ring auf B eingestellt ist und dessen Position auf B eingestellt ist, mit dem Unterschied, dass sich die Umkehrposition um einen Schritt verschiebt, da die Kerbe fixiert ist. Wir werden später sehen, wie sich die Umkehrpositionen auf den Bombe-Prozess auswirken können.

Die Bombe verwendet Trommeln, die Buchstaben auf die gleiche Weise wie die Enigma-Rotoren verschlüsseln. Sie haben jedoch keine Kerbe oder Ringeinstellung. Es gibt immer noch eine Umkehrung, aber sie findet immer an der Position „Y” der Trommeln statt. Die Trommeln sind durch eine charakteristische Farbe gekennzeichnet, wobei jede Farbe einem der Enigma-Rotoren I bis VIII entspricht. Die Trommeln haben eine ähnliche Verdrahtung wie ihre Enigma-Pendants, aber es gibt Unterschiede. Wahrscheinlich versehentlich sind die Trommeln I, II, III, VI, VII und VIII der Bombe den entsprechenden Enigma-Rotoren um einen Buchstaben voraus.
Die Trommel IV ist zwei Schritte voraus, und der Rotor V ist drei Schritte voraus.

Aufbau der Bombe

Die Vorderseite der Bombe verfügt über 36 Trommelbänke, die in drei Reihen zu je 12 Trommelbänken angeordnet sind. Eine Trommelbank besteht aus drei Trommeln, die die drei Rotoren einer Enigma-Maschine darstellen. Die obere Trommel entspricht dem langsamen Rotor ganz links der Enigma-Maschine und die untere Trommel dem Rotor ganz rechts. Beachten Sie, dass eine Trommelbank nicht einer vollständigen Enigma-Maschine entspricht, sondern nur dem Rotor-Scrambler-Teil, einschließlich des Reflektors.

Die Bombe verfügt über drei Steuerlogik-Sets. Diese werden als Ketten bezeichnet. Die drei Ketten bieten dem Bediener die Möglichkeit, drei verschiedene Nachrichten oder Einstellungen gleichzeitig auszuführen, vorausgesetzt, dass die Anzahl der für jede Einstellung erforderlichen Trommelbänke nicht höher als 12 ist.

Auf der Vorderseite befinden sich außerdem drei Anzeigetrommeln, mit denen ein Teil der möglichen Lösung abgelesen werden kann, sobald die Bombe stoppt. Außerdem gibt es einen Start- und einen Stoppknopf zur Steuerung der motorisierten Mechanik.

Der Reflektor der Enigma-Maschine ist als Panel-Anschluss auf einer Seite der Bombe implementiert. Es gibt drei Panel-Anschlüsse, einen für jeden der 12 Trommelbänke.

Auf der Rückseite der Bombe befinden sich mehrere 26-polige Buchsen. Kabel mit 26 Leitern (ein Leiter für jeden Buchstaben des Alphabets) werden verwendet, um die Buchsen je nach der unten beschriebenen Analyse der verschlüsselten Nachricht auf unterschiedliche Weise zu verbinden. Es gibt spezielle Buchsen, die dazu dienen, einen Teststrom in das System einzuspeisen und das Ergebnis anzuzeigen.

Die andere kurze Seite der Bombe verfügt über eine Reihe von Schaltern, mit denen ausgewählt werden kann, in welchen Anschluss der 26-poligen Buchse (welcher Buchstabe) Strom in das System eingespeist werden soll. Außerdem gibt es einige Schalter zur Steuerung des Schrittmechanismus (Carry genannt) der Trommeln auf der Vorderseite.
Schließlich gibt es noch eine Anzeige vom Typ „Briefkasten”, die nach dem Anhalten der Bombe anzeigt, welcher Buchstabe die mögliche Lösung für die aktuell in der Bombe eingestellte Nachricht ist. Ein Hebel links neben der Briefkastenanzeige dient dazu, die Bombe nach dem automatischen Anhalten wieder zu starten.

Erstellen eines Menüs aus einer Vorlage

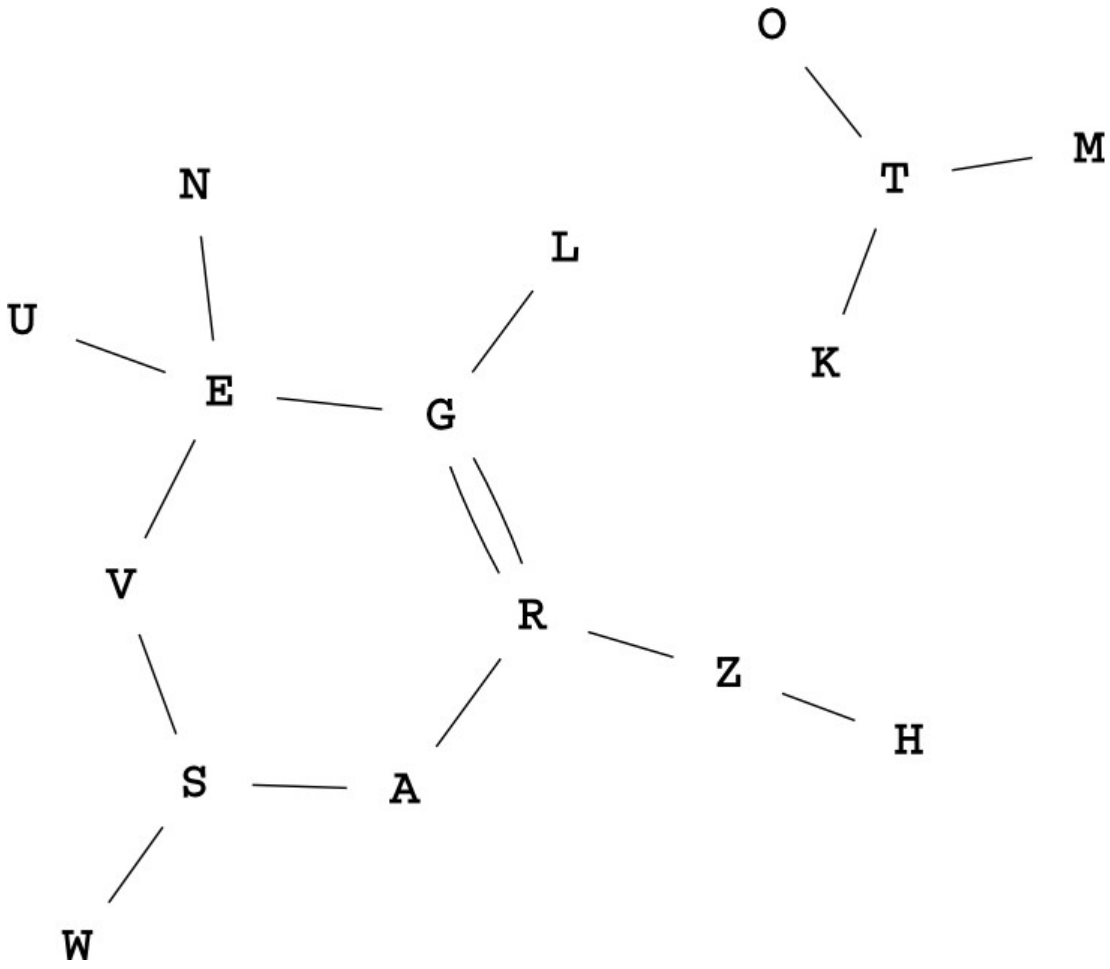
Der erste Schritt beim Versuch, den Schlüssel zur Verschlüsselung einer Nachricht wiederherzustellen, ist die Erstellung eines Diagramms, das als Menü bezeichnet wird. Anhand des Menüs lässt sich erkennen, ob die Nachricht mit der Bombe erfolgreich verarbeitet werden kann. Das Menü gibt auch Auskunft darüber, wie die Kabel auf der Rückseite der Bombe für die betreffende Nachricht angeschlossen werden müssen.
Um ein Menü zu erstellen, benötigen wir einen Teil des Klartexts, der einem Teil der verschlüsselten Nachricht entspricht. Dies wird als Crib bezeichnet. Die Analysten in Bletchley Park wussten, dass viele Nachrichten stereotype Phrasen enthielten, wodurch es möglich war, das Crib zu erraten. Eine weitere hilfreiche Tatsache war, dass eine Enigma-Maschine ein Zeichen nicht in sich selbst verschlüsseln kann, sodass in vielen Fällen sofort erkennbar war, wenn eine stereotype Phrase oder ein stereotypisches Wort an einer bestimmten Position in einer verschlüsselten Enigma-Nachricht fehlte. Wenn sie den Schlüssel für eine einzelne Nachricht finden konnten, die an einem Tag empfangen wurde, konnten sie alle Nachrichten lesen, die an diesem Tag empfangen wurden, da für alle Nachrichten eines Tages in einem bestimmten Enigma-Netzwerk derselbe Schlüssel verwendet wurde.

Als Beispiel für die Erstellung eines Menüs verwenden wir die folgende Crib:

Buchstabe Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Löschen	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E
Chiffre	S	N	M	K	G	G	S	T	Z	Z	U	G	A	R	L	V

WETTERVORHERSAGE ist der Klartext und bedeutet auf Deutsch „Wettervorhersage”.

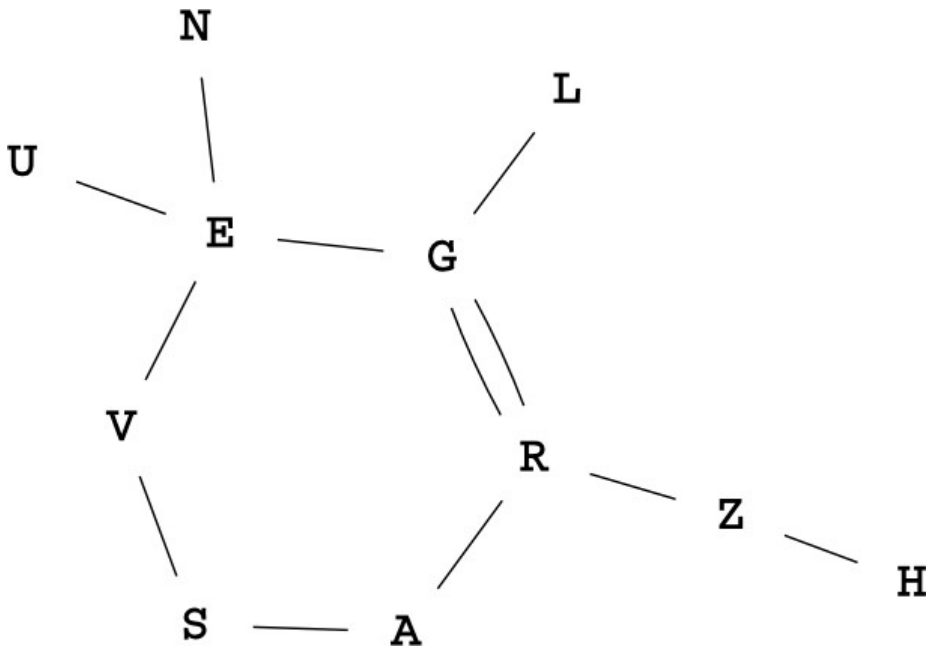
Anschließend zeichnen wir ein Diagramm, in dem Verbindungen zwischen einem verschlüsselten Zeichen und seinem Klartext-Gegenstück hinzugefügt werden.



Das Ziel ist es, einen zusammenhängenden Graphen mit möglichst vielen Schleifen zu erhalten. Wenn ein Menü nicht genügend Buchstaben und/oder Schleifen enthält, kommt es zu vielen Fehlstopps der Bombe, was bedeutet, dass viel Arbeit erforderlich ist, bis wir den richtigen Schlüssel ermitteln können.

Das Menü besteht nun aus zwei getrennten Grafiken, was im Allgemeinen nicht erwünscht ist. Wir entfernen daher die Buchstaben O, T, M, W und K aus unserem Menü. Es ist auch praktisch, nicht mehr als 12 Links in einem Menü zu haben. Wie bereits erwähnt, können wir drei Rotorkonfigurationen gleichzeitig testen, wenn das zu testende Menü höchstens 12 Trommelbänke verwendet. Wir entfernen den Buchstaben W, um nur 12 Links zu erhalten. Durch das Entfernen von W werden keine der beiden Schleifen im Menü unterbrochen.

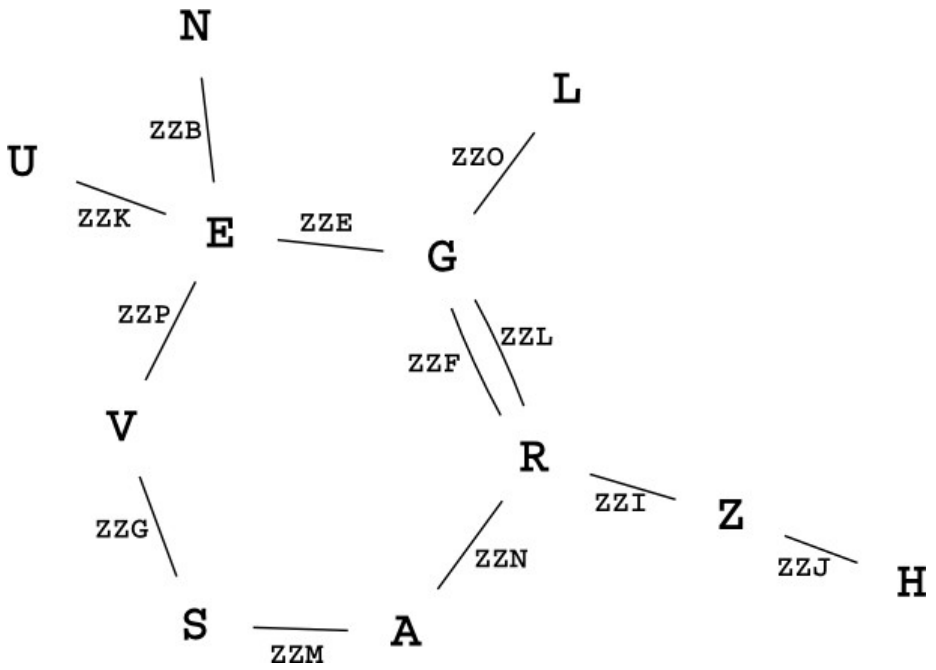
Das Diagramm sieht nun wie folgt aus:



Zu diesem Diagramm fügen wir dann zusätzliche Informationen hinzu. Wir nehmen an, dass die Enigma-Rotoren vor der Verschlüsselung der Nachricht auf ZZZ eingestellt waren und dass kein mittlerer Rotorwechsel stattgefunden hat. Die Bombe betrachtet ZZZ als „Ausgangsposition".

Unter den oben genannten Umständen wäre der erste Buchstabe des Klartexts mit den Enigma-Rotoren in der Position ZZA verschlüsselt worden, der zweite Buchstabe mit ZZB und so weiter. Tragen Sie die vermutete Position der Enigma-Rotoren für jede Verbindung im Diagramm ein.

Das resultierende Diagramm:



Weisen Sie jeder Verbindung im Diagramm eine Trommelbank zu und tragen Sie die Nummer der Trommelbank zusammen mit der angenommenen Rotorposition in eine Tabelle ein. Versuchen Sie, eine fortlaufende Reihenfolge von Trommelbanken zu erhalten, die dem Fluss des Diagramms folgt. Dies vereinfacht die Verdrahtung auf der Rückseite der Bombe, da wir spezielle Brückenverbinder verwenden können, die den Ausgang einer Trommelbank mit dem Eingang der nächsten verbinden.

Wir werden den folgenden Weg durch das Diagramm nehmen, um diesen Effekt zu maximieren: U -> E -> G -> R -
> A -> S -> V -> E -> N und H -> Z -> R -> G -> L.

Wählen Sie einen zentralen Buchstaben im Diagramm aus und bezeichnen Sie ihn als „Eingabe“. Hier wird der Teststrom eingespeist. In diesem Fall wählen wir den Buchstaben G.

Schließlich erstellen wir eine weitere Tabelle, in der wir jeden Buchstaben im Diagramm den Verbindungen zuordnen, die für diesen Buchstaben verwendet werden. Beispielsweise ist U nur mit dem Eingang von Drum Bank 1 verbunden. E hingegen ist sowohl mit dem Ausgang von 1 als auch mit dem Eingang von 2 sowie mit dem Ausgang von 7 und dem Eingang von 8 verbunden. Wenn ein Buchstabe mit dem Ausgang einer Bank und dem Eingang der nächsten verbunden ist, schreiben wir diese Verbindung in Klammern. Dies dient als Erinnerung daran, dass wir für diese Verbindung einen Brückenverbinder verwenden können.

Der letzte Schritt besteht darin, zu entscheiden, welcher Buchstabe getestet werden soll. Es sollte ein Buchstabe sein, der im Menü vorhanden ist, aber nicht derselbe oder neben dem eingegebenen Buchstaben steht. Wir wählen A und schreiben dies im Menü als „Aktuelle Eingabe bei A”.

Damit ist die Erstellung des Menüs abgeschlossen, das nun wie folgt aussehen sollte:

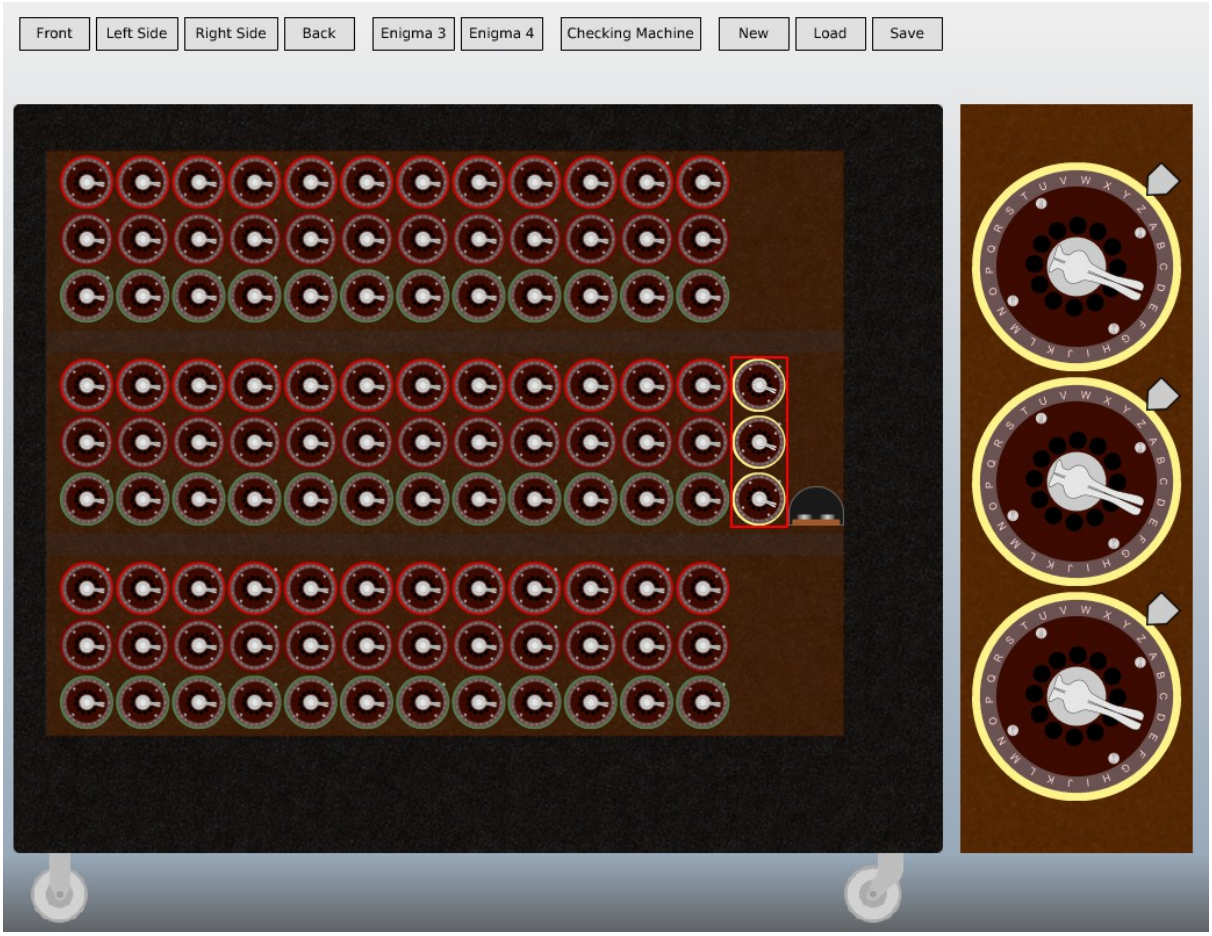
```
1: ZZK
2: ZZE
3: ZZF
4: ZZN
5: ZZM
6: ZZG
7: ZZP
8: ZZB
9: ZZJ
10: ZZI
11: ZZL
12: ZZO

U: 1 rein
E: (1 aus, 2 ein), (7 aus, 8 ein)
G: (2 aus, 3 ein), (11 aus, 12 ein), Eingang
R: (3 raus, 4 rein), (10 raus, 11 rein)
A: (4 raus, 5 rein)
S: (5 raus, 6 rein)
V: (6 raus, 7 rein)
N: 8 raus
H: 9 rein
Z: (9 aus, 10 ein)
L: 12 raus

Aktueller Eintrag bei A.
```

Dieses Menü testet die Hypothese, dass A auf der Stecktafel der Enigma-Maschine mit G verbunden war. Aufgrund der cleveren Konstruktion der Bombe erhalten wir jedoch auch dann die richtigen Stecktafelverbindungen, wenn sich diese Hypothese als falsch herausstellt (was wahrscheinlich ist).

Einrichten des Menüs auf der Bombe



Zuerst wählen wir aus, welche Rotoren wir in welcher Reihenfolge ausprobieren möchten. Da wir nicht mehr als 12 Trommelbänke verwenden, können wir auf Wunsch drei Rotorreihenfolgen gleichzeitig ausprobieren. Vorerst probieren wir jedoch nur eine Reihenfolge aus: II, V, III, die zufällig die richtige ist.

Von vorne gesehen besteht die Trommelbank 1 aus den drei Rotoren ganz oben links, Nummer 2 befindet sich rechts von Bank 1 und so weiter. Wählen Sie die Trommelbank 1 aus, indem Sie darauf klicken. Eine Nahaufnahme der Trommelbank wird auf der rechten Seite des Simulators angezeigt. Drücken Sie die kreisförmige Pfeiltaste neben der Nahaufnahme der Trommeln, bis die richtige Rotorreihenfolge eingestellt ist. II oben, V in der Mitte und III unten. Klicken Sie auf die Schaltfläche „In Kette kopieren", um diese Rotorreihenfolge auf alle Trommelbänke in der oberen Kette (Trommelbänke 1-12) zu übertragen.

Stellen Sie als Nächstes die Trommeln gemäß dem Menü auf die richtigen Buchstaben ein. Die Trommelbank 1 sollte auf ZZK eingestellt sein; drehen Sie die obere Trommel auf Position Z, die mittlere auf Z und die untere Trommel auf K.

Wiederholen Sie diesen Vorgang für die anderen 11 Drum-Bänke und stellen Sie sicher, dass Sie die Drums gemäß dem Menü auf die Buchstaben einstellen.

Standardmäßig ist der Bombe-Simulator so eingestellt, dass er den B-Reflektor verwendet. In einigen Fällen wurden jedoch auch andere Enigma-Reflektoren verwendet. Um dies zu ändern, klicken Sie auf die Schaltfläche „Left Side" (linke Seite) und dann auf

auf den Reflektor-Panel-Anschluss, um ihn zu ändern. In unserem Fall sollten wir ihn so lassen, wie er ist, und Reflektorplatine B verwenden.

Die Verkabelung des Menüs erfolgt auf der Rückseite der Bombe. Klicken Sie auf die Schaltfläche „Zurück“, um eine Abbildung der Buchsen auf der Rückseite der Bombe anzuzeigen. An jede Buchse kann entweder ein 26-poliges Kabel (ein Kabel für jeden Buchstaben im Enigma-Alphabet) oder ein spezieller Brückenverbinder angeschlossen werden. Ein Brückenverbinder verbindet eine Buchse mit der direkt darunter liegenden Buchse und verfügt außerdem über eine eigene Buchse. Die mit „CO1“ gekennzeichneten Buchsen sind alle miteinander verbunden. Das Gleiche gilt für „CO2“ und so weiter.

Zuerst platzieren wir die Brückenverbinder. Diese sollten an den Anschlüssen platziert werden, die wir in Klammern geschrieben haben. Um den Ausgang von Trommelbank 1 mit dem Eingang von Trommelbank 2 zu überbrücken, klicken Sie auf die mit „OUT1“ gekennzeichnete Buchse. Klicken Sie im daraufhin erscheinenden Kontextmenü auf „Neue Brücke“. Wiederholen Sie dies für alle möglichen Brückenpositionen im Menü.

Anschließend verbinden wir das gesamte Menü von oben nach unten, beginnend bei U. Gemäß dem Menü sollte U mit dem Eingang von Drum Bank 1 verbunden werden. Klicken Sie auf die mit U gekennzeichnete Buchse in der linken Spalte der Buchsen. Die drei Spalten mit den Buchsen mit den Bezeichnungen A-Z sind Verbindungen zu etwas, das als Diagonalboard bezeichnet wird. Auf der Bombe gibt es drei Diagonalboards.

Der nächste Buchstabe im Menü, E, ist mit zwei Brücken verbunden. Wir müssen daher einen der gemeinsamen Steckersätze verwenden. Verbinden Sie zunächst den E-Stecker mit einem der mit CO1 gekennzeichneten Stecker, es spielt keine Rolle, mit welchem. Klicken Sie dazu zunächst auf einen der Stecker und wählen Sie „Neues Kabel“. Es erscheint ein Kabel, das den ausgewählten Stecker mit dem nächstgelegenen freien Stecker verbindet. Klicken und ziehen Sie die Anschlüsse des Kabels so, dass es sich von E bis CO1 erstreckt. Erstellen Sie dann ein neues Kabel, diesmal von einer der anderen CO1-Buchsen zur Buchse am Brückenanschluss zwischen OUT1 und IN2. Fügen Sie ein drittes Kabel hinzu, das eine weitere CO1-Buchse mit der Buchse am Brückenanschluss zwischen Bank 7 und 8 verbindet. Damit ist die E-Zeile im Menü fertiggestellt.

Fahren Sie so für alle Buchstaben im Menü fort. Der aktuelle Eingang, den wir unter dem Buchstaben G ausgewählt haben, ist eine der Buchsen mit der Bezeichnung CH. Wählen Sie CH1 als Eingang für dieses Menü.

Klicken Sie auf die Schaltfläche „Right Side“ (rechte Seite). Sie sehen nun einen Bereich auf der rechten Seite mit vielen Schaltern, einem Briefkasten-Display und einem Hebel (neben dem Briefkasten). Es gibt vier Spalten mit Schaltern, eine für jeden Satz von 12 Trommelbänken (Ketten) der Bombe und eine zusätzliche Kette, die für erweiterte Menüs verwendet werden kann. Es gibt einen Ein-/Aus-Schalter für jede Kette und dann einen Schalter pro Buchstabe im Enigma-Alphabet. Damit kann der Benutzer auswählen, in welchen der 26 Anschlüsse (A-Z) ein Teststrom eingespeist werden soll. Um die Schalter unten zu sehen, ziehen Sie das rote Rechteck in der kleinen Ansicht nach links. Unterhalb der A-Schalter befinden sich drei Schalter. „Carry Home” wird verwendet, um den Übertragungsmechanismus auf allen Trommeln zu aktivieren, bis sie sich in der Ausgangs- oder Home-Position befinden. Auf diese Weise kann die Bombe schnell in ihren Ausgangszustand zurückgesetzt werden. „Double Input” wird manchmal zusammen mit der Aux-Kette für erweiterte Menüs verwendet und wird hier nicht weiter erläutert. „Carry“ wird aktiviert, um den regulären Übertragungsmechanismus zu starten, sodass die mittleren Trommeln bei jeder vollständigen Umdrehung der schnellen Trommeln einen Schritt vorrücken und so weiter. Schalten Sie die folgenden drei Schalter ein: „Chain 1“ oben, den Schalter „A“ von Chain 1 und „Carry“ unten.

Betreiben der Bombe

Das Menü ist nun eingerichtet und die Bombe ist betriebsbereit. Auf der Vorderseite der Bombe befinden sich rechts neben den drei goldenen Anzeigetrommeln zwei Tasten. Die linke Taste startet die Bombe. Die rechte Taste stoppt die Bombe. Drücken Sie die Starttaste und beobachten Sie, wie sich die Trommeln drehen. Die Bombe hat nun begonnen, einen Teil des Enigma-Schlüsselraums nach einer Einstellung zu durchsuchen, die dem aktuellen Menü entspricht.

Umgang mit Bombe-Stopps

Es ist wahrscheinlich (und war sogar erwünscht, um zu überprüfen, ob die Bombe ordnungsgemäß funktioniert), dass es mehr als einen Stopp gibt, bevor die Bombe die Suche im aktuellen Teil des Schlüsselraums abgeschlossen hat. Nur einer dieser Stopps ist der richtige Stopp, der dem auf der Enigma-Maschine verwendeten entspricht. Die anderen Stopps sind zufällig und resultieren aus mathematischer Wahrscheinlichkeit. Jeder Stopp muss auf seine Gültigkeit überprüft werden. Dazu verwenden wir die Prüfmaschine.
Wenn die Bombe zum ersten Mal stoppt, zeigen die goldenen Anzeigen SNY an, und das Briefkasten-Display an der Seite der Bombe zeigt den Buchstaben D an. Wir schreiben dies als SNY:D. Sobald der Stopp notiert wurde, kann die Bombe neu gestartet werden, um ihre Suche fortzusetzen. Dazu drückt man zunächst den Startknopf auf der Vorderseite (den linken der beiden Knöpfe) und hebt dann kurz den Hebel links neben der Buchstabenanzeige an der Seite der Bombe an. Während die Bombe weiter sucht, kann der erste Stopp auf der Prüfmaschine getestet werden.

Die Prüfmaschine

Durch Klicken auf die Schaltfläche „Prüfmaschine“ wird eine Ansicht der Prüfmaschine von oben angezeigt. Die Prüfmaschine ähnelt der Enigma, sie verfügt über eine Tastatur, vier Trommeln, einen Reflektor und Lampen, um einen verschlüsselten Buchstaben anzuzeigen. Sie hat jedoch keine Stecktafel und auch keine Mechanismen zum Bewegen der Trommeln.
Auf der linken Seite befindet sich eine Kassette, die als Reflektor fungiert. Sie kann ausgetauscht werden, um verschiedene Reflektoren anzupassen. Da für diese Nachricht der B-Reflektor verwendet wurde und B die Standardeinstellung des Simulators ist, müssen wir dies nicht ändern. Da unsere Nachricht aus einer Enigma mit drei Rotoren stammt, wird ganz links eine Dummy-Trommel mit einer Eins-zu-Eins-Zuordnung der Buchstaben des Alphabets verwendet. Die Dummy-Trommel ist gelb und hat keine Buchstabenmarkierungen. Klicken Sie auf den Pfeil über den anderen drei Trommeln, bis sie wie folgt als Bombe eingerichtet sind: II, V, III (von links nach rechts).
Schreiben Sie die Buchstaben aus dem Menü in einer Spalte auf ein Blatt Papier:

U:
E:
G:
R:
A:
S:
V:
N:
H:
Z:
L:

Stellen Sie als Nächstes die Ringe auf den Trommeln auf die auf dem Anschlag angegebenen Buchstaben ein, in diesem Fall: SNY. Um die Trommelringe einzustellen, halten Sie die Umschalttaste gedrückt, während Sie die Trommel mit der Maus drehen. Wenn Sie ein Touch-Gerät verwenden, können Sie einen Finger an einer beliebigen Stelle auf dem Bildschirm halten, während Sie die Trommel mit einem anderen Finger drehen. Die Ringeinstellung wird durch einen kleinen schwarzen Punkt am äußeren Rand der Trommel angezeigt. Wenn Sie fertig sind, sollten sich die Punkte jeweils neben den Buchstaben S, N und Y befinden.

Die Bombe deutete darauf hin, dass auf der Enigma-Stecktafel der Buchstabe G mit dem Buchstaben D verbunden ist. Schreiben Sie den Buchstaben D neben G.

Wenn wir im Menüdiagramm vom Buchstaben G (unserem ausgewählten Eingabebuchstaben) zum Buchstaben E wechseln möchten, müssen wir die Trommeln auf ZZE einstellen. Drehen Sie die Trommeln an der Prüfmaschine auf ZZE. Wenn wir nun die Taste D drücken (die vorgeschlagene Steckerplatinenverbindung von G, auch Steckerpartner genannt), sehen wir, was der mögliche Steckerpartner von E ist. In diesem Fall leuchtet P auf; schreiben Sie P neben E. Mit diesem neu gefundenen Steckerpartner von E können wir nun die möglichen Steckerpartner für die Buchstaben im Menüdiagramm überprüfen, die mit E verbunden sind, und so weiter. Folgen Sie auf diese Weise jedem Link im Diagramm und notieren Sie sich alle vorgeschlagenen Steckerpartner. Wenn Sie zu einem Buchstaben gelangen, für den Sie bereits einen Steckerpartner haben, sollte derselbe Buchstabe das Ergebnis sein. Ist dies nicht der Fall, ist diese Station falsch und wir müssen zurück zur Bombe gehen und eine neue finden. Denken Sie daran, dass ein Buchstabe sehr wohl sich selbst als Steckerpartner haben kann. Dies entspricht einem nicht verbundenen Buchstaben auf der Steckertafel der Enigma und wird manchmal als selbstgesteckter Buchstabe bezeichnet.

Das vollständige Ergebnis für diesen Stopp sollte wie folgt aussehen:

```
U: W
E: P
G: D
R: P
A: X
S: Q
V: I
N: T
H: H
Z: X
L: O
```

Hier haben wir zwei Widersprüche: X kann nicht sowohl mit Z als auch mit A verbunden sein, und P kann nicht mit E und R verbunden sein.

Dieser Stopp ist daher falsch.

Der nächste Stopp der Bombe sollte DKX:Q sein. Wiederholen Sie den Vorgang auf der Prüfmaschine, diesmal mit den Ringen auf der Prüfmaschine auf D, K, X eingestellt, und der vorgeschlagene Steckerpartner unseres Eingabebuchstabens G im Menü ist nun Q. Sobald alle Verbindungen im Diagramm getestet sind, sollte das Ergebnis lauten:

```
U: F
E: T
G: Q
R: R
A: D
S: S
V: N
N: V
H: M
Z: P
L: J
```

In diesem Fall gibt es keine Widersprüche. Stattdessen ist es beruhigend, dass V N als Steckerpartner hat und N V. Dieser Stopp, DKX:Q, besteht den Test und ist es wert, weiter untersucht zu werden. Auch wenn wir keine Widersprüche gefunden haben, besteht die Möglichkeit, dass es sich dennoch nicht um die richtige Lösung handelt.

Den Enigma-Nachrichtenschlüssel erhalten

Um einen möglichen Schlüssel weiter zu untersuchen, verwenden wir eine Simulation einer echten Enigma-Maschine. Klicken Sie auf die Schaltfläche „Enigma 3”. Daraufhin wird eine Simulation einer Enigma mit drei Rotoren von oben angezeigt. Oben rechts neben der Enigma-Maschine befindet sich eine Box mit Ersatzrotoren und einem weiteren Reflektor. Unter der Rotorbox befindet sich ein Bereich, in dem beim Tippen klare und verschlüsselte Buchstaben angezeigt werden.
Zuerst richten wir die Enigma-Maschine so ein, wie wir es derzeit für richtig halten. Klicken Sie auf den grau-roten Knopf, der sich entweder links neben der P-Lampe oder rechts neben der L-Lampe befindet. Dadurch wird der Deckel „abgeschraubt“ und die Enigma geöffnet. Klicken und ziehen Sie den Rotor, bis die richtigen Rotoren II, V und III von links nach rechts an ihrem Platz sind.
Als Nächstes stellen wir die Ringeinstellungen auf DKX. Drücken Sie zunächst die Taste „Set Rings“, um den Ringeinstellungsmodus zu aktivieren. Klicken Sie nun auf einen installierten Rotor und ziehen Sie ihn nach oben oder unten, um die Ringe auf D, K bzw. X einzustellen.
Schließen Sie den Deckel der Enigma, indem Sie erneut auf einen der beiden grau/roten Knöpfe drücken. Stellen Sie die Startposition des Rotors auf ZZZ ein, indem Sie jeden Rotor nach oben oder unten ziehen.
Als Nächstes verbinden wir die uns bekannten Einstellungen der Stecktafel. Klicken Sie auf die Stecktafelanschlüsse, die am unteren Rand der Enigma-Maschine zu sehen sind. Dadurch sollten Sie eine Vorderansicht der Stecktafel selbst erhalten. Direkt unter der Stecktafel stehen zehn Kabel zur Verfügung. Verbinden Sie diese gemäß den Ergebnissen der Maschinenprüfung: U mit F, E mit T und so weiter. Buchstaben, die mit sich selbst verbunden werden sollten (R und S), sollten nicht verbunden werden. Der Standardzustand eines Buchstabens ist, dass er mit sich selbst verbunden ist.
Wenn alle Kabel angeschlossen sind, klicken Sie auf eine Taste der Enigma-Tastatur (oben zu sehen), um zur Draufsicht auf die Enigma-Maschine zurückzukehren.

Um die zuvor erwähnten Fehler auf den Bombe-Trommeln (*siehe Seite 2*) auszugleichen und da wir die Rotoren II, V und III verwenden, übersetzen wir unsere angenommene Startposition ZZZ in YWY.

Versuchen wir nun, die Nachricht zu entschlüsseln! Nehmen Sie mit der Startposition YWY die Position eines Enigma-Operators ein, der eine verschlüsselte Nachricht empfängt. Geben Sie den Chiffretext SNMKGGSTZZUGARLV ein. Das Ergebnis ähnelt dem gewünschten, ist aber nicht ganz richtig: WETCERVXRHERSAGE. Das C und das X sind nicht die erwarteten Buchstaben. Dies liegt höchstwahrscheinlich daran, dass wir noch nicht alle Stecktafelverbindungen kennen.
Schauen wir uns zunächst C an. Wir haben versucht, den Buchstaben K zu entschlüsseln und erhielten C anstelle des erwarteten Buchstabens
T. Wir könnten dann möglicherweise den gewünschten Buchstaben T erhalten, indem wir ein Kabel zwischen C und T auf der Stecktafel verbinden. Allerdings ist T bereits mit einem Kabel verbunden – mit E. Unsere nächste Strategie besteht also darin, einen Buchstaben zu finden, der allein durch die Rotoren an der Rotorposition dieses Buchstabens (ZZD in Bombe-Rotoren) zu E verschlüsselt würde. Da E mit T verbunden ist, würde dies zum gewünschten Ergebnis führen. Gehen Sie zurück zur Prüfmaschine und stellen Sie die Trommeln auf ZZD ein. Drücken Sie die Tasten auf der Tastatur, bis Sie den einen Buchstaben finden, der zu E verschlüsselt wird. Dieser Buchstabe ist I. Verbinden Sie auf der Stecktafel I und K mit einem Kabel.
Beim nächsten Problem haben wir ein X erhalten, wollten aber ein O. Weder X noch O sind mit einem Kabel verbunden. Verbinden Sie das letzte Kabel zwischen X und O.
Setzen Sie die Enigma auf YWY zurück und versuchen Sie erneut, den Chiffretext zu entschlüsseln. Wir erhalten nun das erwartete Ergebnis: WETTERVORHERSAGE.

Alle Buchstaben in unserer Crib sind nun korrekt entschlüsselt. Bedeutet das, dass wir den richtigen Schlüssel haben? Ja und nein. Da wir alle zehn Steckbrettpaare haben, ist dieser Teil des Rätsels höchstwahrscheinlich gelöst (vorausgesetzt, unsere beiden Vermutungen sind richtig). Aber die Ringeinstellung und die Startpositionen der Rotoren sind wahrscheinlich nicht ganz korrekt.
Wenn wir einen längeren Abschnitt des Chiffretextes hätten als nur den Teil der Crib (was normalerweise der Fall sein dürfte), dann wäre zu erwarten, dass der zu entschlüsselnde Text irgendwann von verständlichem Text zu Kauderwelsch wechseln würde. Wenn ein solcher plötzlicher Wechsel von Klartext zu verschlüsseltem Text auftritt, kann man davon ausgehen, dass der linke und/oder mittlere Rotor einen Schritt weitergedreht wurde, obwohl dies nicht hätte geschehen dürfen. Dies kann entweder auf „unserer" Seite geschehen sein oder beim ursprünglichen Chiffrierbeamten, aber nicht bei uns. Wenn wir vermuten, dass eine Umstellung an der falschen Position stattgefunden hat, können wir den Ring und die Startposition Schritt für Schritt anpassen, bis wir die richtige Kerbenposition gefunden haben. Im schlimmsten Fall müssen wir dies 25 Mal pro Rotor tun, es handelt sich also nicht um einen übermäßig schwierigen Vorgang. Es ist zu beachten, dass der in diesem Dokument beschriebene Vorgang nicht funktioniert, wenn eine Umstellung in der Mitte der Crib stattfindet.

Zusammenfassung

Wir haben nun ein Beispiel dafür gesehen, wie eine verschlüsselte Enigma-Nachricht mit Hilfe einer Crib-Datei entschlüsselt werden kann. Aus der Crib-Datei wurde ein Menü erstellt, das dann zur Einrichtung der Bombe für die betreffende Nachricht verwendet wurde. Die Bombe-Stopps wurden in der Prüfmaschine überprüft, und der vielversprechende Stopp wurde in einer Enigma-Maschine weiterverarbeitet, um einen vollständigeren Schlüssel zu erhalten.
Wir haben ein wenig geschummelt, da wir im Voraus wussten, welche Rotoren und Reflektoren verwendet wurden und in welcher Reihenfolge die Rotoren in der Enigma montiert waren. In der Praxis wäre dasselbe Menü verwendet worden.

auf mehreren Bomben eingerichtet. Mit drei Ketten auf der Bombe war es möglich, drei verschiedene Rotorfolgen auf einer Bombe zu überprüfen.
Dieser Vorgang musste jeden Tag und für jedes Enigma-Netzwerk, das von Interesse war, wiederholt werden.
Es war viel Arbeit erforderlich, um dies Tag für Tag, Woche für Woche aufrechtzuerhalten. Aber die in Bletchley Park gewonnenen Informationen waren so wertvoll, dass sie den Krieg schätzungsweise um mindestens zwei Jahre und wahrscheinlich sogar um vier Jahre verkürzt haben!

Übung

Hier ist eine mit Enigma verschlüsselte Nachricht, die Sie mit der in diesem Dokument beschriebenen Methode entschlüsseln können:

QATCTQCNWMTVCOPYVFHOLCQTVGMTWOBRFOUBRMQBRIHLLXDBTZLXLGZUQFC
WPXPOKOLFFADXDAVTJM

Hilfe: SECRETMESSAGE
Rotoren: II I III