Friedrich-Schiller-Universität Jena
Fakultät für Mathematik und Informatik

Didaktik der Informatik, Modul B

Ausarbeitung 2

Ein Werkzeugkasten zur Enigma

Alexander Johannes 64686

Stefan Uthe 92780

29. Januar 2009

Betreuer: Prof. Dr. Michael Fothe

Inhaltsverzeichnis

1. Einleitung

Ziel dieser Ausarbeitung ist es zum Einen, die Enigma in den historischen Zusammenhang einzuordnen. Zum Anderen werden Werkzeuge vorgestellt, die ein Begreifen der einzelnen technischen Aspekte der Enigma fördern.

1.1. Historie der Enigma

Das Prinzip des Rotors zur Verschlüsselung von Botschaften wurde vor 1920 von vier verschiedenen Personen unabhängig voneinander zum Patent angemeldet. Dazu zählt unter anderem der Deutsche Arthur Scherbius (1878-1929) mit seiner Enigma, die er 1918 zum Patent anmeldete (vgl. Bauer, 1997; S. 107-108 [1]). Die Enigma wurde seit 1923 in verschiedenen Modellvarianten kommerziell beworben und vertrieben, bevor sie ab 1928 durch das deutsche Militär evaluiert, erweitert und standardisiert wurde. Im Zuge dessen verschwand sie dann relativ schnell vom Markt (vgl. Kruh & Deavours, 2002 [2]; Singh, 2001; S. 175-178 [3]). Das deutsche Militär ließ bis zum Ende des zweiten Weltkrieges mehr als 30000 Exemplare der Enigma in verschiedenen Ausfertigungen bauen. Eingesetzt wurde sie nicht nur im Militär, sondern auch bei der Polizei, Geheimdiensten, Diplomaten, Reichspost und Reichsbahn.
Mit dem Einsatz der Enigma begannen die Bemühungen anderer Staaten, die verschlüsselten Funksprüche der Deutschen zu dechiffrieren. In den Anfangsjahren bis 1939 erzielten hauptsächlich polnische Kryptologen um Marian Rejewski (1905-1980) Erfolge bei der Entschlüsselung. Sie stützten sich auf Unterlagen zur Enigma, die der Deutsche Hans-Thilo Schmidt (1888-1943) 1931 an Frankreich verkaufte. Die Polen waren dadurch in der Lage, die Enigma mit 3 Walzen und einer Umkehrwalze nachzubauen. Die Repliken wurden im *Cyklometr* und der *Bomba* verwendet, um den verwendeten Tagesschlüssel zu ermitteln. So war es ab 1937 möglich, die empfangenen Funksprüche relativ problemlos zu entschlüsseln. An seine Grenzen stieß Rejewski, als eine zweite Umkehrwalze und zwei weitere Rotoren auf deutscher Seite hinzukamen (vgl. Singh, 2001; S. 179-199 [3]; Bauer, 1997; S. 391-399 [1]).
Kurz vor dem Einmarsch der Deutschen in Polen erhielten Frankreich und Großbri-

tannien das erworbene Wissen, um die Entschlüsselung weitertreiben zu können. Auf britischer Seite sind besonders die Verdienste von Alan Turing (1912-1954) und Gordon Welchman (1906-1985) hervorzuheben. Sie entwickelten, gestützt auch auf die polnische Vorarbeit, die *Bombe*, welche auf elektromechanischen Weg alle Walzenstellungen und -lagen durchtestete, um den verwendeten Schlüssel eines Funkspruches zu ermitteln. Dies geschah immer auf der Basis von Annahmen über den Klartext. Durch die Mechanisierung wurde es überhaupt erst möglich, Nachrichten zeitnah entschlüsseln zu können (vgl. Singh, 2001; S. 211-219 [3]; Bauer, 1997; S. 400-409 [1]). Die USA bauten, basierend auf den britischen Plänen, weitere Hochleistungsversionen der *Turing-Welchman-Bombe*, welche hauptsächlich gegen die 4-Rotoren-Enigma der deutschen Kriegsmarine eingesetzt wurden (Bauer, 1997; S. 409-412 [1]).
Die Enigma spielte in den strategische Überlegungen des deutschen Militärs eine tragende Rolle, da sie eine sichere Kommunikation einzelner Einheiten ermöglichte. Dies wurde häufig zur Koordinierung von Angriffen auf gegnerische Stellungen genutzt. Durch mangelnde Sorgfalt beim Umgang mit der Enigma (Zeichenverdopplungen, leicht zu erratende Walzenstellungen, stereotype Wendungen im Klartext etc.) und konstruktive Unzulänglichkeiten (involutorische Verschlüsselung, besondere Charakteristiken jeder Walze etc.) wurde es möglich, die Verschlüsselung kontinuierlich zu brechen. Dies legte einen der Grundsteine für den Sieg der Allierten über Deutschland und das Ende des zweiten Weltkrieges (vgl. Singh, 2001; S. 228-230 [3]).

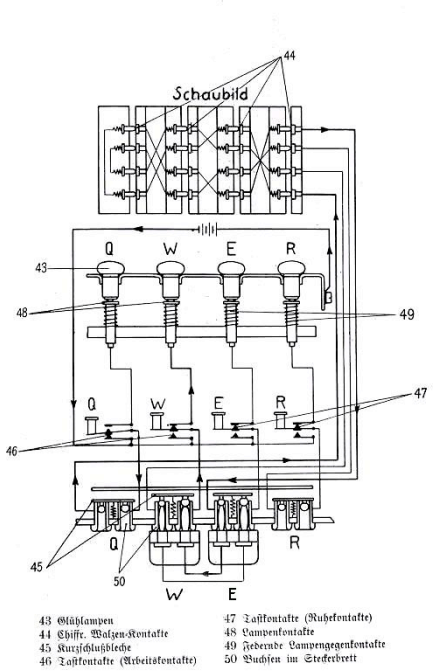
1.2. Überblick zum Aufbau der Enigma

Die Enigma wurde in verschiedenen Varianten eingesetzt. Abbildung 1.1 (a) zeigt das gebräuchlichste Modell mit Steckerbrett, Tastenfeld, Lampenfeld und drei Walzen. Abbildung 1.1 (b) veranschaulicht die elektrische Verdrahtung, ausgehend von einer Taste durch das Steckerbrett, die drei Walzen, die Umkehrwalze, zurück durch die drei Walzen, das Steckerbrett, hin zu einer Lampe.

1.3. Der Werkzeugkasten

Der Werkzeugkasten enthält drei verschiedene Modelle und Simulationen der Enigma. Die Walzen und damit das Prinzip einer Rotorchiffriermaschine werden in Kapitel 2 am Beispiel eines Papiermodells beschrieben. Kapitel 3.2 erläutert Tasten- und Lampenfeld, sowie die elektische Funktionsweise anhand eines Modells. Auf das

(a) Enigma



(b) schematischer Aufbau

Abbildung 1.1.: Die Enigma und ihr schematischer Aufbau

Steckerbrett wird in Kapitel 4 im Zusammenhang mit einem Simulator eingegangen. An jedem der Werkzeuge wird ein Teilaspekt der Enigma erläutert. Zudem wird für jedes Werkzeug eine Anleitung zum Nachbau und zur Inbetriebnahme gegeben. Abschließend werden für jedes Werkzeug Möglichkeiten des Einsatzes im Informatikunterricht aufgezeigt und Beispielaufgaben beziehungsweise Interaktionen mit dem Modell beschrieben.

2. Papiermodell

2.1. Prinzip der Rotorchiffriermaschine und der Verschlüsselung

Ein Rotor (im weiteren als Walze bezeichnet) ist ein Zylinder mit einer festen Anzahl an elektrischen Kontakten an den beiden Stirnseiten. Die Kontakte sind kreisförmig entlang des Randes angebracht und im Inneren der Walze miteinander verbunden. Eingangs- und Ausgangskontakt sind in der Regel nicht geradlinig verbunden. Bei einer Rotorchiffriermaschine liegen mehrere Walzen auf einer gemeinsamen Rotationsachse nebeneinander, so dass sich die Kontakte berühren. Jede Walze kann unabhängig von den anderen gedreht werden. Die Lage der Walzen zueinander wird im Laufe der Verschlüsselung geändert.
Zur Vereinfachung werden die Eingangs- und Ausgangskontakte der Walzenreihung mit Buchstaben bezeichnet.
Wird ein Signal an einen Eingangsbuchstaben angelegt, läuft es zunächst durch die Walze zum verbundenen Kontakt. Dieser liegt an einem Kontakt der Nachbarwalze. So breitet sich das Signal durch die Walzenreihe bis zum Ausgangsbuchstaben aus. Nach der Kodierung eines Buchstabens werden die Walzen gegeneinander verdreht. Dies geschieht nach einem festen Schema.
Durch das Ändern der Walzenstellung nach jedem Verschlüsselungsschritt werden gleiche Eingangsbuchstaben nicht auf gleiche Ausgangsbuchstaben abgebildet. Dadurch wird eine polyalphabetische Substitution vorgenommen.
Zum Dekodieren werden Ein- und Ausgang der Walzenreihung vertauscht und für jeden Buchstaben die korrekte Walzenlage eingestellt.
In der Praxis wird die Anfangsstellung der Walzen meist aus einem Codebuch entnommen, welches Sender und Empfänger besitzen. In der Regel dreht sich die Eingangswalze bei jedem Verschlüsselungsschritt eins weiter. Die nachfolgenden Walzen werden dann wie bei einem Kilometerzähler an einer bestimmten Stelle um einen Schritt mitgenommen.
Die Enigma besaß die Besonderheit der Umkehrwalze, die sich am Ende der Wal-

zenreihung befand. Dadurch wurde das Signal nach dem Durchlaufen der Walzen wieder zurück durch die Walzenreihung geschickt. Dies hatte den Vorteil, dass Sender und Empfänger die gleiche Walzenreihenfolge und -lage zum Kodieren und Dekodieren verwenden konnten. Die Verschlüsselung war involutorisch und es wurde kein Buchstabe auf sich selbst abgebildet.

2.2. Aufbau und Funktion des Modells

Das Papiermodell (siehe Anhang B.1) besteht aus drei Walzen, einer Umkehrwalze und einem Buchstabenring. Dies werden ausgeschnitten und jeweils zu Ringen zusammengeklebt. Zur leichteren Benutzung können die Ringe auf eine Papröhre geschoben werden. Durch die Linien auf den Walzen lässt sich sehr leicht der Signalweg vom Buchstabenring über die Walzen, durch die Umkehrwalze und zurück durch die Walzen zum Buchstabenring verfolgen.
Um die Anschaulichkeit zu erhöhen, besitzt das Papiermodell nur sechs Buchstaben. Am Wort *RENNEN* wird die Funktionsweise des Papiermodells erläutert. Die Walzen werden in der Reihenfolge *U - III - II - I - E* verwendet. In der Grundstellung liegen alle Buchstaben *E* in einer Linie. Nun wird der Signalweg von *R* vom Buchstabenring aus verfolgt. Am Ende des Signalweges steht der Buchstabe *E*. Nach dem Drehen der ersten Walze um einen Schritt liegen nun die Buchstaben *EEERE* in einer Linie. Nun wird der zweite Buchstabe *E* kodiert: *S*. Am Ende erhält man die kodierte Buchstabenfolge *ESEISE*. Die Dekodierung ist durch Einstellen auf die Grundstellung sofort möglich.

```
RENNEN
ESEISE
```

An der Kodierung der aufeinanderfolgenden Buchstaben *NN* durch *EI* und der Abbildung der Buchstaben *R* und *N* (am Ende) auf *E* lässt sich gut die polyalphabetische Substitution erkennen.

2.3. Aufgabenstellungen

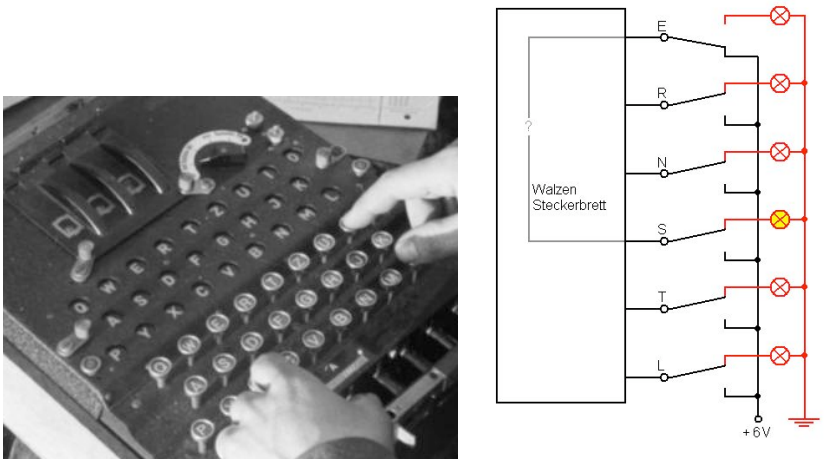
Das Papiermodell eignet sich hervorragend, um die prinzipielle Funktionsweise der Enigma im Unterricht zu behandeln. Der Signalweg kann direkt mit dem Finger verfolgt werden. Wichtig ist es, den Schülern das Weiterdrehen der Walzen genau zu erklären, da dies beim Papiermodell die meiste Aufmerksamkeit erfordert.

Wenn die Schüler mit dem Umgang vertraut sind, teilt man die Klasse in Gruppen und gibt an jede Gruppe einen Geheimtext aus. Zudem bekommt jede Gruppe die Reihenfolge der Walzen und die Anfangslage mitgeteilt. In Anhang B.2 sind einige kurze Sätze aus der Buchstabenfolge *ERNSTI* aufgeführt, die dann später zu einer Geschichte durch die Schüler zusammengesetzt werden können.
Weiterhin können sich die Schüler selbst Wörter und Sätze ausdenken, die sich mit den vorhandenen Buchstaben bilden lassen. So kann eine Gruppe Nachrichten verschlüsseln und einer anderen Gruppe zum entschlüsseln weitergeben.
Das Aufdecken eines Geheimnisses motiviert die Schüler. Durch die unterschiedlichen Sätze wird die Neugier geweckt, welche was herauskommt, wenn man die Ergebnisse der Gruppen zusammenfügt. Stärkere Gruppen können im Laufe der Gruppenarbeit weitere Geheimtexte bekommen. Das *Begreifen* der Walzen und der aktive Umgang mit dem Modell festigt so ganz automatisch das Wissen über die Funktionsweise der Rotorverschlüsselung am Beispiel der Enigma.

3. Modell

3.1. Funktion von Tastenfeld und Lampen

An dem Modell kann vor allem die interne Funktion des Tasten- und Lampenfeldes der Enigma beobachtet werden. Der Schüler erhält hier einen direkten Einblick in die Verdrahtung und kann quasi unmittelbar, am Kabel entlang, die Schaltung *begreifen*.



(a) Tastenfeld (b) Schaltung

Abbildung 3.1.: Das Tasten- und Lampenfeld

Das Lampenfeld und die Tastatur bilden zusammen die Ein- und Ausgabeeinheit der Enigma. Die Tasten der Enigma fungieren dabei als Zwei-Wege-Schalter. Ungedrückte Tasten werden von einer Feder in Verbindung mit dem Kontakt, der mit den Lampen und der Masse verbunden ist, gehalten. Drückt man nun ein Taste wird Kontakt zur Stromquelle hergestellt. Der Strom kann nun in das Steckbrett und danach in die Walzen fließen und kommt dann an einem der Ausgänge B-F heraus und fließt über die Glühlampe und die Masse ab, die Lampe leuchtet auf und der chiffrierte Buchstabe (hier: D) kann abgelesen werden (Abb. 3.1 (b)). Dabei kann es nicht zu einem Kurzschluss kommen, da die Chiffrierung der Enigma keinen Buchstaben auf sich selbst abbildet.

3.2. Weg des Stromes

Der Weg des Stroms durch die Enigma ist eine weiterer Aspekt der sich mit Hilfe des Enigmamodells erklären lässt. Über die Funktion der einzelnen Komponenten wurde in den zugehörigen Kapiteln geschrieben, aber es ist wichtig sie in den Gesamtzusammenhang der Schaltung einzuordnen. Abbildung A.1 im Anhang A zeigt den Weg des Stromes als roten Pfad. Zunächst fließt der Strom von der Quelle zur gedrückten Taste. Von dort aus geht es weiter zum Steckerbrett dann in die rechte Walze, mittlere Walze, linke Walze und schließlich in die Umkehrwalze. Aus dieser geht es wieder in umgekehrter Reihenfolge durch die Walzen. Danach fließt der Strom zurück zum Steckerbrett, dann durch den ungedrückten Taster des Geheimtextbuchstabens durch die zu ihm gehörende Glühlampe. Schlussendlich fließt der Strom über die Masse ab, bis die Taste losgelassen wird.

3.3. Aufbau und Funktion des Modells

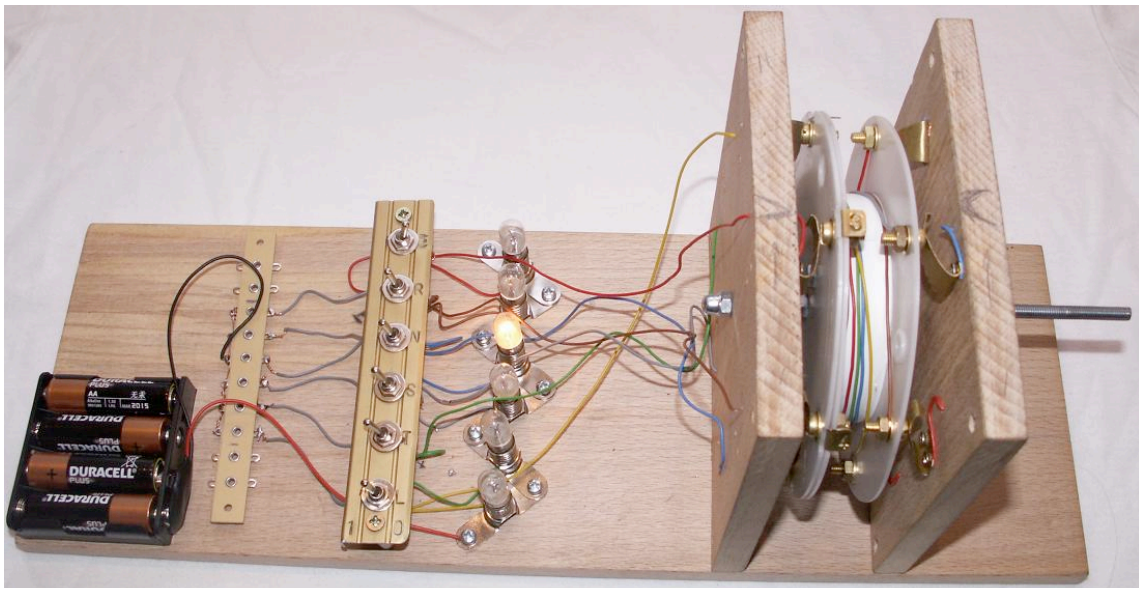


Abbildung 3.2.: Das Modell

Das Modell besteht aus sechs Schaltern und Glühlampen, einer Walze und einer feststehenden Eingangs- und Umkehrwalze. Als Stromversorgung dienen vier AA-Batterien. Die Funktionsweise und Verdrahtung entspricht dem Schema der originalen Enigma. Abbildung 3.2 gibt einen Eindruck vom Modell, Anhang C enthält die Bauanleitung.

3.4. Aufgabenstellung

Durch die offene Bauweise und die farbigen Kabel des Enigmamodells lässt sich der Weg des Stroms leicht verfolgen.
Eine Beispielaufgabe könnte folgendermaßen lauten:
Vollziehe den Weg des Signals durch das Modell der Enigma nach. Zeichne den Weg, den der Strom nimmt, in die vorgegebene Skizze ein. Trage auch die Schalterstellungen ein.
Das Experiment kann nun mehrmals mit dem selben Buchstaben, aber veränderter Walzenstellung vorgenommen werden. Der Schüler soll dabei bemerken, dass durch die Rotation der Strom immer einen anderen Weg nimmt. Dies ergibt trotz der nicht wechselnden Verdrahtung, mehrere Alphabete.

4. Simulator

4.1. Funktion des Steckerbrettes

Das Steckerbrett für die Enigma wurde erstmals bei der „Wehrmachts-ENIGMA“ von 1934 eingeführt. Reichsbahn, Reichspost und Polizei benutzten jedoch weiterhin die unsicherere Version ohne Steckerbrett.

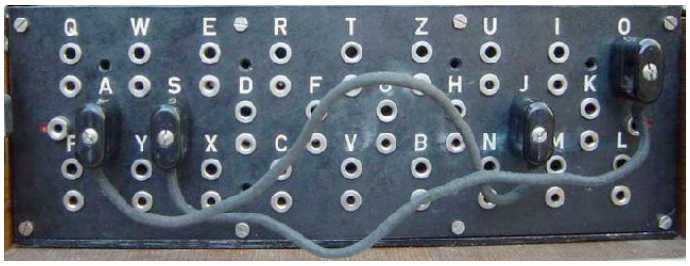


Abbildung 4.1.: Das Steckerbrett der Enigma

In Abbildung 4.1[1] sieht man, dass die Doppelbuchsen in drei Reihen und in der selben Reihenfolge, wie auf der Tastatur angeordnet waren.

4.1.1. Aufbau

Für jeden Buchstaben des Alphabets besaß das Steckerbrett der Enigma eine Buchse mit je zwei Kontakten. Die dazugehörigen Kabel hatten Stecker mit zwei Stiften. Wenn kein Stecker eingesteckt wurde, waren beide Buchsen elektrisch miteinander verbunden. Mit eingesteckten Stecker wurden jeweils zwei Buchsen über Kreuz verbunden. Dies ist in Abbildung 4.2 gut sichtbar.
So führt das Einstecken eines Kabels zur Vertauschung der beiden Buchstaben und damit zu einer monoalphabetischen Substitution. Diese ist involutorisch, das bedeutet, dass das Kodieren und Dekodieren auf gleiche Weise erfolgt. Der Effekt des Steckerbretts auf die Schlüssellänge ist gigantisch, auf die Komplexität der Entschlüsselung jedoch nur gering.

[1] Quelle: http://de.wikipedia.org/wiki/Enigma_(Maschine)

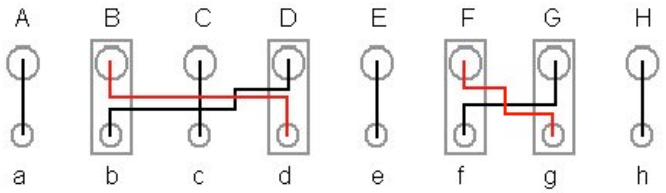


Abbildung 4.2.: Schema der Verkabelung

4.1.2. Das Steckerbrett des Simulators

Im Steckerbrett des Simulators können bis zu zehn Steckerverbindungen realisiert werden. Im Original sind zwar bis zu 13 möglich, jedoch wurden nie mehr als zehn in der Praxis verwendet. Will man zwei Buchsen verbinden, stellt man einfach in einer der zehn Spalten in der oberen Zeile den Buchstaben der einen und in der unteren Zeile den Buchstaben der anderen Buchse ein. Welches Zeichen dabei oben und welches unten steht, ist wegen der Involutorik des Sytems egal. Stehen gleiche Buchstaben in einer Spalte, oder kommt der Buchstaben gar nicht in den Fenster vor, entspricht das einem gezogenen Stecker. Wichtig ist, dass Buchstaben pro Zeile höchstens einmal und pro Spalte höchstens doppelt vorkommen dürfen (Abb. A.2).

4.2. Einsatz der Enigma

Der Simulator ist hervorragend dazu geeignet, den Schülern die Benutzung der Chiffriermaschine näher zu bringen und somit ein Stück Geschichte nachzuerleben.

4.2.1. Tages- und Spruchschlüssel

Sender und Empfänger einer verschlüsselten Nachricht müssen sich auf eine gemeinsame Einstellung der Enigma einigen, um ungehindert miteinander kommunizieren zu können. Zum Tagesschlüssel gehören die Nummern, Reihenfolge, Ring- und Anfangsstellung der verwendeten Walzen und die Vertauschungen am Steckerbrett. Die Tagesschlüssel wurden in Schlüsselbüchern verteilt und waren streng geheim.
In der Anfangsphase der militärischen Nutzung der Enigma wurde der Tagesschlüssel erst für 3 Monate gültig, später dann für einen Monat. Erst ab dem 01.10.1936 wurde er schließlich jeden Tag gewechselt. Ab Mitte 1942 ging man zum achtstündigen Schlüsselwechsel über.
Jeder Funkspruch wurde mit einem Spruchschlüssel verschlüsselt. Dieser bestand aus

den drei Buchstaben einer selbstgewählten Grundstellung der Walzen. Der Spruchschlüssel wurde mit dem Tagesschlüssel verschlüsselt und der Nachricht vorangestellt. Da der Tagesschlüssel nur zur Chiffrierung des Spruchschlüssels verwendet wurde, war die gefunkte Datenmenge, die einen Angriff auf den Tagesschlüssel zuließ, sehr klein. Der eigentliche Nachrichtentext wurde ja mit einem zufälligen Spruchschlüssel verschlüsselt. Allerdings wurde der Spruchschlüssel bis 1939 zweimal hintereinander geschrieben und diese sechs Zeichen dann verschlüsselt. Dies gab den polnischen Kryptologen die entscheidende Angriffsmöglichkeit gegen die Enigma.

4.2.2. Umwandlung des Klartextes

Da es keine Leertaste auf der Enigma gibt, wurden einfach alle Leerzeichen entfernt. Zahlen wurden ausgeschrieben. Die Satzzeichen wurden durch *X* ersetzt, Umlaute wurden mit *E* markiert und *CH* durch *Q* ersetzt. Zudem wurden Eigennamen verdoppelt und in *X* gesetzt. Zur Erleichterung der Lesbarkeit teilte man den so normierten Klartext in Fünfergruppen auf.
Hierzu ein kurzes Beispiel:

```
Das Oberkommando der Wehrmacht verkündet: Die Stadt Jena
ist nicht mehr zu halten, um 24 Uhr Rückzug einleiten.
```

Spruchschlüssel *BUMBUM* und normierter Klartext:

```
BUMBUM

DASOB ERKOM MANDO DERWE HRMAQ TVERK UENDE TXDIE STADT XJENA XJENA
XISTN IQTME HRZUH ALTEN XUMVI ERUND ZWANZ IGUHR RUECK ZUGEI NLEIT
ENX
```

4.2.3. Verschlüsseln

Zunächst sieht der Chiffreur in das Schlüsselbuch und liest den Tagesschlüssel für das aktuelle Datum ab (Tabelle 4.1).
Als erstes wird die Ringstellung der verwendeten Walzen eingestellt. Dazu verdreht man den Buchstabenring jeder Walze gegenüber der Verdrahtung. Danach werden die Walzen in der vorgegebenen Reihenfolge eingesetzt und das Steckerbrett verkabelt. Der Simulator kann analog zu der Vorgehensweise eingerichtet werden.
Als nächstes werden die Walzen auf die Grundstellung gebracht und der gewählte Spruchschlüssel zweimal eingegeben. Die sechs Zeichen werden an den Anfang der

Datum	Umkehr-walze	Walzenlage	Ring-stellung	Grund-stellung	Steckerverbindungen
30.	B	I II III	01 08 03	21 14 05	AJ BN DP IH JK ZO QE LS YX VF
29.	B	III IV V	10 11 12	02 17 04	FI CD KQ VL OX YZ EH UJ PM NB
28.	B	V II I	23 03 16	11 03 12	KV ZI QU XA EG FR CT NM PS YD

Tabelle 4.1.: Tagesschlüssel

Nachricht gesetzt. Danach werden die Walzen auf den Spruchschlüssel eingestellt und die Nachricht eingegeben und notiert.
Für das Beispiel wird der Tagesschlüssel vom 30. verwendet. So ergibt sich folgender Geheimtext:

```
GAHQSL

AIFGQ ACDZV KYXKU YGSZP GEFBB CSSEL QOCUU ZTZEJ MNXGJ NTUXO DNNGQ
NZYZU LWBUP RHPJM TUINY KNPCY WUZHI IHIJN XXCQD LYHIN VIOTR PGCKJ
OST
```

Der Geheimtext wurde zusammen mit der Uhrzeit, der Nachrichtenlänge und einer Kenngruppe zur Kennzeichnung des Empfängers gemorst.
Zum Dechiffrieren wurde der selbe Vorgang durchgeführt. Die Einstellungen der Enigma waren gleich, da der Dechiffrierende den gleichen Tagesschlüssel benutzte.

4.2.4. Anmerkungen und Fazit

Die Bedienung der Enigma ist ein wichtiger Aspekt für den Informatikunterricht, denn er zeigt wie wichtig die richtige Bedienung für die Sicherheit eines Chiffrierverfahrens ist. Anhand der Verdoppelung des Spruchschlüssels und der feststehenden Wendung *Das Oberkommando der Wehrmacht verkündet:* kann gut auf die Problematik der Klartext/Geheimtextkompromittierung eingegangen werden.

4.3. Aufgabenstellung

Vorausgesetzt wird, dass die Schüler mit der Verwendung der Original-Enigma vertraut sind. Es ist günstig diese Aufgabe zu stellen, wenn gerade die Zeit des Zweiten Weltkrieges im Unterricht behandelt wird.

Es wird ein Rollenspiel durchgeführt.
Gruppen und Materialien: Es werden drei Teams gebildet. Zunächst benötigen wir drei Schüler für das Team *Sender*, einen Chiffreur, seinen Assistenten, einen Funker und einen Lastwagenfahrer. Das zweite Team, *Empfänger*, besteht aus Assistent, Funker und Chiffreur. Das dritte Team *Gegenseite* besteht aus Abhörer, Kommandant (der Lehrer) und dem Saboteur. Als Material werden benötigt: Zettel mit *A-Stadt*, *B-Stadt* und *Autobahn 1* bedruckt, zwei Rechner mit dem Enigmasimulator, einen Pappkarton mit der Aufschrift *Nachschub* und ein Paar Papierzettel.
Vorbereitung: Der äußerste linke Rechner im Computerkabinett wird mit *A-Stadt* bezeichnet, der äußerste rechte Rechner mit *B-Stadt*. Auf dem Gang dazwischen wird der Zettel mit *Autobahn 1* gelegt.
Ablauf: Der Chiffreur des Teams *Sender* bekommt folgenden Ausdruck und Tagesschlüssel:

```
Streng Geheim! Folgendes an Team Empfänger senden: „Haltet durch!
Wir schicken unverzüglich Nachschub über die Autobahn 1."
```

Datum	Umkehr-walze	Walzenlage	Ring-stellung	Grund-stellung	Steckerverbindungen
xx.	B	I II III	01 08 03	21 14 05	AZ BN DP IO

Mit diesen Informationen kodiert der Chiffreur den Text, nach den Regeln aus Abschnitt 4.2.2 (um Zeit zu sparen und nicht zu sehr auf unwesentlichen Details zu verharren, gibt der Lehrer Hilfestellung). Sein Assistent notiert den Geheimtext auf einen Zettel und übergibt ihn dem Funker. Dieser ruft einen Buchstaben nach dem anderen dem Funker des Teams *Empfänger* zu, dieser notiert den Text. Gleichzeitig schreibt auch der *Abhörer* mit. Nun diktiert der Assistent dem Chiffreur des Teams *Empfänger* den Text. Hat das Team den Text erfolgreich dekodiert, geben sie den Funkspruch „verstanden“ durch. Nun erhält der Lastwagenfahrer den *Nachschub* und transportiert ihn von *A-Stadt* nach *B-Stadt*. Er bleibt dabei unbehelligt vom Saboteur, weil der Abhörer ohne Enigma und Tagesschlüssel mit dem Funkspruch nichts anfangen kann.
Das Szenario wird wiederholt, diesmal erhält das Team *Gegenseite* jedoch einen Neuzugang, den Kryptoanalytiker. Er besitzt die Karte „Mathematische Methoden der Kryptoanalyse, Spionageergebnisse, Bomba“. Alles verläuft wie gehabt, nur dass diesmal der Abhörer die abgefangene Nachricht an den Kryptoanalytiker weiterleitet. Dieser erhält durch seine Karte den Klartext der verschlüsselten Nachricht vom Spielleiter. Diese Erkenntnis gibt er an den Kommandanten weiter, dieser wiederum

veranlasst den Saboteur mit einem Stuhl die *Autobahn 1* zu blockieren. Der Transport wird verhindert und das Team *Empfänger* zieht sich aus *B-Stadt* zurück.
Abgeschlossen wird das Rollenspiel mit einer Diskussion. Zentrale Fragen könnten dabei sein:
Welche Auswirkungen hatte die Existenz von Institutionen wie dem Biuro Szyfrów und Bletchley Park auf den Verlauf die Dauer des Krieges? Welche Schlussfolgerungen zum Thema Datensicherheit im Alltag lassen sich daraus ziehen?

4.4. Entwurf des Simulators

4.4.1. Benutzeroberfläche

Abbildung A.2 zeigt die Benutzeroberfläche des Simulators. Oben links ist das Lampenfeld (1) zu sehen. Ein grüner Punkt erscheint in dem Feld, der zu dem entsprechenden Geheimtextbuchstaben gehört. Unter (2) ist die Tastatur der Enigma zu sehen. Die Anordnung der Tasten Entspricht der des Originals. Jeder eingegebene Buchstabe wird, um den Überblick zu wahren, im Eingabetextfeld (3) verzeichnet. Der durch die Maschine chiffrierte bzw. dechiffrierte Buchstabe wird im Ausgabetextfeld (4) verzeichnet. Beim Übernehmen der Einstellungen mit der Taste *Start* werden auch die Inhalte der Felder gelöscht. Das Kodieren und Dekodieren wird im Abschnitt 4.2 *Einsatz der Enigma* beschrieben.

4.4.2. Module und objektorientierte Aspekte des Entwurfs

Der Entwurf des Simulators orientiert sich so nah wie möglich am Aufbau der Enigma. Es wurde der objektorientierte Ansatz gewählt mit den Modulen *Steckerbrett* und *Walze*. Die Implementierung erfolgte in Java. Die Quellen finden sich in Anhang D, eine lauffähige Version auf der beiliegenden CD.
Das Modul *EnigmaModul* beschreibt einen generischen Baustein in der Enigma. Es besitzt die Methoden *kodieren*, *nachLinksKodieren*, *nachRechtsKodieren* und *zählen*. Zudem existieren die Attribute *vorher*, *nachher*, *zaehler* und *verdrahtung*.
Steckerbrett und *Walze* sind von *EnigmaModul* abgeleitet und implementieren die einzelnen Methoden. Die Umkehrwalze unterscheidet sich nur durch die Verdrahtung von den anderen Walzen. Über die Attribute *vorher* und *nachher* wird eine doppelt verkettete Liste aufgebaut.
Die Liste wird immer nach dem Schema *Steckerbrett* $\Leftrightarrow$ *Walze 1* $\Leftrightarrow$ *Walze 2* $\Leftrightarrow$ *Walze 3* $\Leftrightarrow$ *Umkehrwalze* aufgebaut. Um einen Buchstaben zu kodieren, wird die

Methode *kodieren* des *Steckerbretts* aufgerufen. Diese führt die Kodierung durch und ruft mit dem Ergebnis die Methode *kodieren* des im Attribut *nachher* referenzierten *EnigmaModuls* auf. So führt das Kodieren eines Zeichens zu dem Aufrufstapel in Tabelle 4.2.

Aufruf	mit dem Wert von	Richtung
Steckerbrett.kodieren	Eingabe	links
Walze1.kodieren	Steckerbrett.nachLinksKodieren	links
Walze2.kodieren	Walze1.nachLinksKodieren	links
Walze3.kodieren	Walze2.nachLinksKodieren	links
Umkehrwalze.kodieren	Walze3.nachLinksKodieren	links
Umkehrwalze.kodieren	Umkehrwalze.nachLinksKodieren	rechts
Walze3.kodieren	Umkehrwalze.nachRechtsKodieren	rechts
Walze2.kodieren	Walze3.nachRechtsKodieren	rechts
Walze1.kodieren	Walze2.nachRechtsKodieren	rechts
Steckerbrett.kodieren	Walze1.nachRechtsKodieren	rechts

Tabelle 4.2.: Aufrufstapel beim Kodieren eines Zeichens

Zuerst wird die Methode *zaehlen* der ersten Walze aufgerufen. Dies bewirkt das Fortschalten der Walze um eine Position. Wenn die Nut zur Weiterschaltung erreicht ist, wird *zaehlen* der nachfolgenden Walze aufgerufen. Nach dem Weiterschalten aller Walzen wird zunächst nach links kodiert bis zur Umkehrwalze und danach nach rechts kodiert.
An diesem Beispiel ist die Ausnutzung der Polymorphie sehr gut ersichtlich. Alle Objekte in der verketteten Liste sind vom Typ *EnigmaModul*. Erst zur Laufzeit wird die jeweils korrekte Methode zum Kodieren von Steckerbrett oder Walze aufgerufen. Somit kann der Entwurf des Simulators im Unterricht mit zur Vermittlung der objektorientierten Konzepte Vererbung und Polymorphie eingesetzt werden.

A. Abbildungen

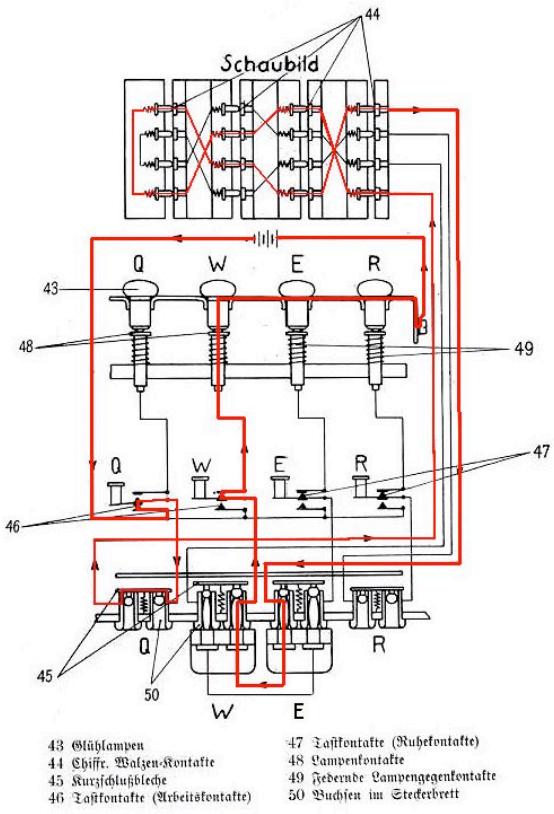


Abbildung A.1.: Der Weg des Stromes

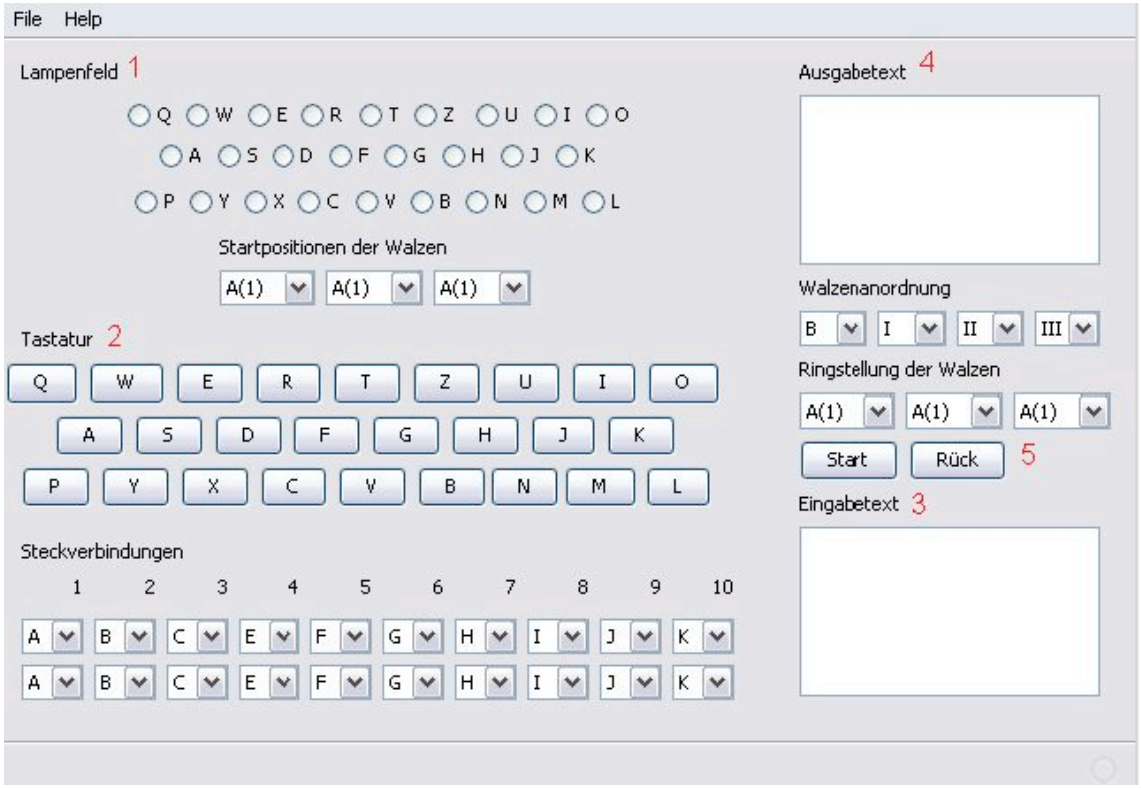


Abbildung A.2.: Benutzeroberfläche des Simulators

B. Papiermodell

B.1. Bastelbogen

Siehe nächste Seite.

B.2. Wörter und Sätze der Buchstabenkombination „ERNSTI“

B.2.1. Wörter

EI, EIER, EIERN, EIN, EINE, EINEN, EINER, EINERSEITS, EINES, EINNISTEN, EINREISEN, EINREISSEN, EINREISST, EINRENNE, EINS, EINSEN, EINSER, EINST, EINSTEIN, EINTRETE, EINTRETEN, EINTRITST, EINTRITT, EINTRITTE, EINTRITTEN, EINTRITTS, EIS, EISEN, EISENS, EISENSTEIN, EISERN, EISERNE, EISERNER, EISERNES, EISES, EISTEE, EITER, EITERN, EITERT, EITERTE, ENTE, ENTEISE, ENTEISEN, ENTEIST, ENTEISTE, ENTEISTER, ENTEISTES, ENTEISTEST, ENTEN, ENTENEIER, ENTENTE, ENTERE, ENTERN, ENTERT, ENTERTE, ENTERTEN, ENTREISSE, ENTREISSEN, ENTREISST, ENTRINNST, ENTRISS, ENTRISSEN, ENTRISSENE, ENTRISSENEN, ENTRISSENES, ENTRISSEST, ENTRISSET, ENTSINNE, ER, ERINNERE, ERINNERN, ERINNERST, ERINNERT, ERINNERTE, ERINNERTEN, ERINNERTES, ERINNERTEST, ERINNERTET, ERNENNE, ERNENNER, ERNENNST, ERNENNT, ERNST, ERNSTE, ERNSTEN, ERNSTER, ERNSTERE, ERNSTEREN, ERNSTERES, ERNSTES, ERNSTESTE, ERNSTESTEN, ERNSTESTER, ERNSTESTES, ERNTE, ERNTEN, ERNTET, ERNTETE, ERNTETEN, ERNTETES, ERNTETEST, ERNTETET, ERRETTE, ERRETTEN, ERRETTER, ERRETTERIN, ERRETTERN, ERRETTERS, ERRETTEST, ERRETTET, ERRETTETEN, ERRETTETER, ERRETTETES, ERRIET, ERRIETEN, ERRIETEST, ERSINNE, ERSINNEN, ERSINNST, ERSINNT, ERST, ERSTE, ERSTEN, ERSTENS, ERSTER, ERSTERE, ERSTEREN, ERSTERER, ERSTERES, ERSTES, ERSTSERIE, ES, ESS, ESSE, ESSEN, ESSER, ESSERN, ESST, ET, ETERNIT, IN, INNE, INNEN, INNENSEITE, INNER, INNERE, INNEREI, INNEREIEN, INNEREN, INNERER, INNERES, INNERN, INNERST, INNERSTE, INNERSTEN, INNERSTES, INNERT, INS, INSERENT, INSERENTEN, INSERIEREN, INSERIERT, INSERIERTE, INSERIERTER, INSERIERTES, INSERIERTEST, INSISTIEREN, INSISTIERT, INSISTIERTE, INST, INTERESSE, INTERESSEN, INTERESSENT, INTERESSENTEN, INTERESSES, INTERESSIERE, INTERESSIEREN, INTERESSIERST, INTERESSIERT, INTERESSIERTE, INTERESSIERTEN, INTERESSIERTER, INTERESSIERTES, INTERESSIERTEST, INTERN, INTERNE, INTERNEN, INTERNER, INTERNES, INTERNIEREN, INTERNIERT, INTERNIERTE, INTERNIST, INTERSSIERTE, IRE, IREN, IRIN, IRIS, IRR, IRRE, IRREN, IRRER, IRRES, IRRITIERE, IRRITIEREN, IRRITIERST, IRRITIERT, IRRITIERTEN, IRRITIERTER, IRRITIERTEST, IRRITIERTET, IRRSINN, IRRSINNS, IRRST, IRRSTEN, IRRSTER, IRRT, IRRTE, IRRTEN, IRRTEST, ISIS, ISST, IST, ITERIEREN, NEIN, NEISSE, NENNE, NENNER, NENNERS, NENNST, NENNT, NESS, NESSIE, NEST, NESTER, NESTERN, NETT, NETTE, NETTEN, NETTER, NETTEREN, NETTERER, NETTES, NETTESTE, NETTESTER, NETTESTES, NIE, NIENTE, NIERE, NIEREN, NIESE, NIESEN, NIEST, NIESTE, NIESTEN, NIESTEST, NIET, NIETE, NIETEN, NIETETE, NISTE, NISTEN, NISTET, NISTETE, NISTETEN, NISTETET, NITRIEREN, NITRIERT, NITRIERTE, NITRIERTES, NITRIT, NR, NTT, REIN, REINE, REINEN, REINER, REINERE, REINEREN, REINERER, REINERES, REINES, REINSTE, REINSTEN, REINSTER, REINSTES, REIS, REISE, REISEN, REISSE, REISSEN, REISSER, REISST, REISSTE, REISSTEN, REISSTEST, REISSTET, REIST, REISTE, REISTEN, REISTET, REITE, REITEN, REITER, REITEREI, REITEREIEN, REITERIN, REITERINNEN, REITERN, REITEST, REITET, REN, RENITENT, RENN, RENNE, RENNEN, RENNER, RENNST, RENNT, RENTE, RENTIER, RENTIEREN, RENTNER, RENTNERS, RESISTENT, RESISTENTE, RESISTENTEN, REST, RESTE, RESTES, RESTS, RETTE, RETTEN, RETTER, RETTERN, RETTERS, RETTEST, RETTET, RETTETE, RETTETEN, RIES, RIESE, RIESEN, RIESENSTERN, RIESENTIER, RIESENTIERE, RIESIN, RIET, RIETE, RIETEN, RIETET, RIETST, RINNE, RINNEN, RINNSTEIN, RINNSTEINE, RINNSTEINES, RINNT, RINNTE, RISS, RISSE, RISSEN, RIST, RITEN, RITT, RITTE, RITTER, RITTERN, RITTERSTERN, RITTEST, SEE, SEEN, SEEREISE, SEEREISEN, SEES, SEESEITE, SEESTERN, SEESTERNE, SEESTERNEN, SEESTERNS, SEETIER, SEETIERE, SEETIEREN, SEI, SEIEN, SEIN, SEINE, SEINEN, SEINER, SEINERSEITS, SEINES, SEINS, SEIST, SEIT, SEITE, SEITEN, SEITENS, SENNER, SENNEREI, SENNEREIEN, SENSE, SENSEN, SEREN, SERIE, SERIEN, SET, SETTERS, SIE, SINN, SINNE, SINNEN, SINNES, SINNIERE, SINNIEREN, SINNIERST, SINNIERTE, SINNIERTEN, SINNIERTES, SINNIERTEST, SINNIERTET, SINNST, SINNT, SINTER, SINTERN, SINTERS, SIR, SIRENE, SIRENEN, SISTIERE, SISTIEREN, SISTIERST, SISTIERT, SISTIERTE, SISTIERTER, SISTIERTES, SISTIERTEST, SITTE, SITTEN, STEIN, STEINE, STEINEN, STEINERN, STEINERNE, STEINERNER, STEINERNES, STEISS, STERN, STERNE, STERNEN, STERNES, STERNS, STET, STETE, STETEN, STETER, STETES, STETS, STETTIN, STIER, STIERE, STIEREN, STIERST, STIERTE, STIERTEN, STIERTEST, STIESS, STIESSE, STIESSET, STIRN, STIRNE, STIRNEN, STIRNSEITE,

STIRNSEITEN, STREIT, STREITEN, STREITER, STREITEREIEN, STREITERINNEN, STREITERN, STREITERS, STREITET, STREITS, STRESS, STRITT, STRITTEN, TEE, TEER, TEERE, TEEREN, TEERS, TEERST, TEERT, TEERTEN, TEERTEST, TEERTET, TEINT, TEINTS, TENNE, TENNEN, TENNESSEE, TENNIS, TERRIER, TERRINE, TERRINEN, TESSIN, TEST, TESTE, TESTEN, TESTER, TESTEST, TESTET, TESTETE, TESTETEN, TESTIERE, TESTIEREN, TESTIERST, TESTIERT, TESTIERTE, TESTIERTER, TESTIERTES, TESTRENNEN, TESTS, TIER, TIERE, TIEREN, TIERES, TIERRESTEN, TIERS, TINTE, TITRIEREN, TITRIERT, TITRIERTE, TNT, TRENN, TRENNE, TRENNEN, TRENNST, TRENNT, TRENNTE, TRENNTEN, TRENNTEST, TRENNTET, TRENSE, TRENSEN, TRESEN, TRETE, TRETEN, TRETER, TRETERN, TRIEST, TRIST, TRISTEN, TRITT, TRITTE, TRITTEN

B.2.2. Mögliche Sätze und Wortkombinationen

ERNST ERNTETE REIS.

ER RITT EINEN STIER.

IRIS REITET EIN RENTIER.

ER IST EIN RITTER.

IRIS TRITT IN EINEN RINNSTEIN.

ES IST TRIST.

EIN RENTNER REIST IN TENNESSEE.

EINSTEIN ISST EIER.

ERNST IST IN STRESS.

EIER IN NESTERN.

SEI STETS INTERESSIERT!

EIN IRRER ERSINNT EINEN SINN.

EIN RIESE REITET EINEN STIER.

EIN SEESTERN SINNIERT IN SEINEN NESTERN.

EIN RENTNER INSERIERT EIN STEINERNES RIESENTIER.

ER STIERTE IN EINEN SEE.

SIRENEN SIND INTERESSANT.

EIN INTERNIST ISST EINE NIERE.

IN STETTIN IST EIN STEINERNER SEESTERN.

EINNISTEN INS NEST.

SIE TRENNT EIN EI.

TIERE: STIER, RENTIER, SEESTERN

NIE TIERE: RENTNER, RITTER, RIESEN

C. Bauanleitung Modell

Diese Anleitung stellt die wichtigsten Tipps und Punkte zum Bau eines Enigma-Modells mit einer Walze und sechs Buchstaben. Im Mittelpunkt stehen die prinzipiellen Schritte, die je nach ihrem vorliegenden Material und handwerklichen Fähigkeiten angepasst werden können.

C.1. Benötigte Materialien und Werkzeug

- Holzbrett (bevorzugt Hartholz) Stärke zirka 10 – 15mm; Länge ca. 800mm; Breite ca. 150 mm
- Draht in 6 verschiedenen Farben
- Batteriegehäuse 4 * 1,5 V
- 6 Glühlampen 6V mit passender aufschraubbarer Fassung
- 6 Drei-Wege-Schalter
- 2 Scheiben (ca. CD-Durchmesser, je größer, desto besser, aber nicht breiter als das Brett) aus Plastik oder Holz
- 1 Gewindestange (z.B. M5)
- 1 Marmeladenglasdeckel oder ähnlicher flacher Zylinder
- Messingblech ca. 240*100 mm
- 3 Mechanikschrauben mit passenden Muttern
- 7 kurze Holzschrauben (10-15 mm) mit Rundkopf um die Lampen anzuschrauben
- 28 kurze Holzschrauben mit Senkkopf für die Federbleche und das Batteriegehäuse
- 12 kurze Maschinenschrauben mit je zwei Unterlegscheiben und Mutter für die Kontakte der Walze
- Holz- oder Metallleiste für die Schalterhalterung, 2 kurze Rohrstücke als Abstandshalter

- Kunstharz, Lötzinn

Werkzeug
Bohrmaschine, Bohrer; Schraubendreher und Schraubenschlüssel; Blechschere; Kneifzange; Abisolierzange; Lötkolben; Hammer, Körner (und Buchstabenstanzer); Zirkel, Lineal und Bleistift; Eisensäge; Feile, Schleifpapier
Zeit und Geld
Sollten Sie alle Werkzeuge zu Hause haben, benötigen Sie ca. 20-30 € für das Material. Die Bauzeit kostet Sie zirka ein Wochenende.

C.2. Zusammenbau

Die Walze

1. Nehmen Sie die beiden Scheiben und zeichnen sie sich den Mittelpunkt ein. Von diesem Mittelpunkt ziehen Sie mit dem Zirkel einen Kreis mit ca. 5 mm kleinerem Durchmesser als die Scheibe selbst. Zeichnen Sie mit dem Zirkel die Eckpunkte eines gleichseitigen Sechsecks am Kreis ab (einfach sechs mal den Radius abtragen).

   Jetzt wird ein zweiter Kreis mit halbem Durchmesser des Marmeladenglasdeckels aufgezeichnet, auf diesem konstruiert man die Eckpunkte eines gleichseitigen Dreiecks (Abb. C.1 (d)).

   Gießen sie den Marmeladendeckel mit dem Kunstharz aus (alternativ Holzscheibe benutzen).

2. In den Mittelpunkt der Scheiben und des Marmeladendeckels bohren sie ein Loch mit dem Durchmesser der Gewindestange (die spätere Achse der Walzen).

   Bohren sie Löcher mit dem Durchmesser der Schrauben für die Walzenkontakte an den Eckpunkten des Sechsecks. Die drei Löcher auf dem inneren Kreis nehmen später die Maschinenschrauben auf, die die Walze zusammenhalten.

   Kerben Sie ein der Scheiben über den Löchern ein, damit dort später eine Feder einrasten kann.

3. Schrauben Sie die Teile mit den drei dafür vorgesehenen Maschinenschrauben zusammen und trennen sie eventuell überstehendes Gewinde ab.

4. Schneiden Sie aus dem Messingblech 6 rechteckige Stücke der Größe 7*15 mm zu und bohren Sie auf der einen Seite ein Loch mit dem Durchmesser der kleinen Schraube für die Kontakte. Stanzen sie die Zahlen 1 - 6 in die Bleche. Diese markieren später die Stellung der Walze. Wenn Sie keine Stanzen besitzen, können sie die Zahlen auch mit einem wasserfesten Stift aufzeichnen.

5. Bringen Sie die Schrauben und Bleche wie im Bild an, zwischen Unterlegscheibe und Mutter wird das Kabel geklemmt. Die Kabel realisieren die Substitution des Eingabesignals. Sie verbinden jeweils eine Schraube auf der linken mit einer auf der rechten Seiten. Ich habe so verdrahtet (erst linke, dann rechte Seite): 1-2, 2-4, 3-6, 4-3, 5-1, 6-5 (Abb. C.1 (g))

Die Holzteile

Schneiden Sie zwei gleichgroße Teile, die etwas länger als der Durchmesser ihrer Walze sind, vom Brett ab. Diese halten später links und rechts die Achse, auf der die Walze sitzt und erfüllen die Funktion der Eingangswalze (links der Walze) und der Umkehrwalze (rechts der Walze). Bohren Sie in diese Holzteile je ein Loch für die Achse und je sechs Löcher für die Kabel (im selben Sechseck wie auf der Walze angeordnet).
Der übrige Teil des Brettes dient der Enigma als Grundplatte.

Eingangswalze und Umkehrwalze

1. Jeder dieser Teile braucht 6 Schleifkontakte. Diese realisiert man mit Federblechen aus Messing. Diese sollten etwa 20mm breit sein und so lang, das sie einen sicheren Kontakt mit den Schrauben der Walze erlauben (siehe Bild). Versehen sie die Bleche mit zwei Löchern und schrauben Sie sie mit den kurzen Holzschrauben ein gutes Stück in Drehrichtung der Walze (vom Bediener weg) vor den Bohrungen für die Kabel an. Die Löcher für diese Schrauben sollten vorgebohrt werden. Stecken Sie die Kabel durch die Bohrungen und wickeln Sie sie um eine der Schrauben zwischen Blech und Holz. Ziehen Sie alle Schrauben gut fest und biegen sie die Bleche über die Schraubenköpfe (Abb. C.1 (e)).

2. Bei der Umkehrwalze verbinden die Kabel jeweils zwei Kontakte. Die hier verwendete Verdrahtung: oben Mitte – oben links(blau), oben rechts – unten rechts(rot), unten Mitte – unten links (grün)

3. Bei der Eingangswalze werden sechs verschiedenfarbige Kabel angeklemmt.

Die Grundplatte

1. Befestigen Sie das Batteriegehäuse mit 4 Schrauben.

2. Bringen Sie kurze Kabelstücke an den Schrauben an der Unterseite der Lampenfassungen an.

3. Schrauben Sie die Lampen in einer Doppel-“W“ Anordnung auf der Grundplatte mit den Rundkopf-Holzschrauben an, Verbinden Sie die Lampenhalterung über eine Schraube mit dem Batteriegehäuse.

Die Schalterleiste

1. Verlöten Sie den rechten Anschluss der Schalter mit der entsprechenden Lampe, den mittleren mit dem der Lampe entsprechenden Kabel der Eingangswalze und den linken mit der Stromquelle. Zur besseren Übersicht habe ich eine Verteilerbrücke gelötet.

2. Sägen Sie die für die Schalterhalterung vorgesehene Leiste auf die Breite der Grundplatte zu und bohren sie sechs Löcher für die Schalter und zwei für die Schrauben, die die Leiste auf der Grundplatte befestigen. Um die Leiste im richtigen Abstand über der Grundplatte zu halten, werden zwei Alurohrstücke auf 20 mm Länge zugesägt. Schrauben Sie nun die Schalter auf die Leiste und die Leiste auf die Grundplatte. Auch hier wurden Buchstaben und Markierungen für die Schalterstellungen eingestanzt (Abb. C.1 (f)).

Letzte Handgriffe

1. Verbinden Sie die Walze mit der Gewindestange, schrauben Sie so viele Muttern oder Unterlegscheiben auf die Achse bis der Abstand zu den Halterungen groß genug ist. Schrauben Sie Eingangswalze und Umkehrwalze auf die Achse und sägen Sie die überstehenden Enden der Gewindestange ab. Jetzt müssen Sie noch die Holzplatten der Eingangs- und Umkehrwalze von unten an die Grundplatte schrauben.

2. Zusätzlich können Sie noch eine Einrastfeder einbauen oder ein Kurbel befestigen, aber ich möchte mich hier auf die wesentliche Schritte beschränken. Das Enigma Modell ist so einsatzbereit.

C.3. Hinweise zur Benutzung

1. Grundstellung: alle Schalter sind auf „Lampe“ geschaltet (hier: links), Startstellung der Walze oben zu sehen.

2. Nur der Schalter des Buchstabe, der kodiert werden soll, wird auf „Strom“ geschaltet (hier: rechts).

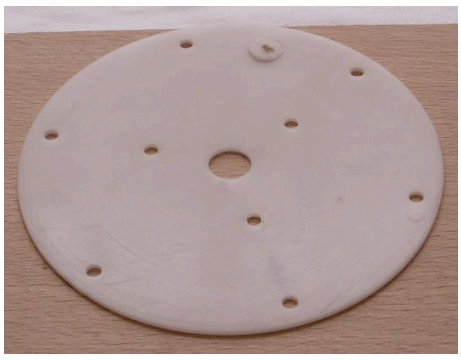
3. Um den nächsten Buchstaben zu kodieren bringt man die Schalter wieder auf Grundstellung und dreht die Walze um eine Position von sich weg (z.B. erst war „1“ oben abzulesen jetzt „2“). Wenn alle Kontakte der Walze die Federbleche berühren, kann man den Schalter für den nächsten Buchstaben umlegen.

4. Schritt drei wiederholen bis der gesamte Klartext kodiert ist (Geheimtextbuchstaben entspricht der leuchtenden Lampe). Das Dekodieren funktioniert genauso wie das kodieren.

(a) Lampe

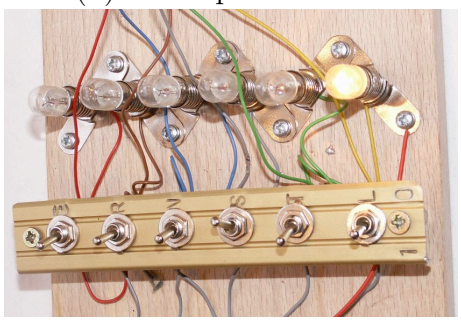
(b) Schalter

(c) Schleifkontakt

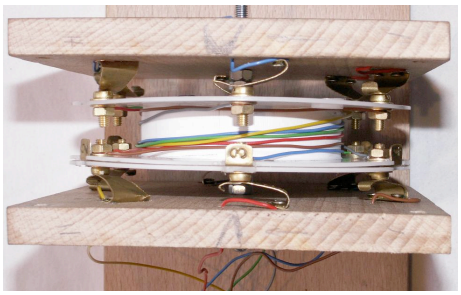


(d) Grundplatte Walze

(e) Grundplatte Umkehrwalze



(f) Schalter und Lampen



(g) Walzen

Abbildung C.1.: Das Modell

D. Quelltexte Simulator

D.1. EnigmaModul.java

```
/* Generische Klasse mit den Methoden kodieren, nachLinksKodieren
   nachRechtsKodieren und zaehlen.*/

package enigmasim;

import java.lang.*;

public class EnigmaModul {
    public EnigmaModul vorher;
    public EnigmaModul nachher;
    public Integer zaehler;
    public int[] verdrahtung;
    public int[] nachRechtsVerdrahtung;

    public EnigmaModul(EnigmaModul vorher,
                       EnigmaModul nachher,
                       int zaehler,
                       int[] verdrahtung) {
        this.vorher = vorher;
        this.nachher = nachher;
        this.zaehler = zaehler;
        this.verdrahtung = verdrahtung;
        this.nachRechtsVerdrahten();
    }

    public void nachRechtsVerdrahten() {
    /* zum einfacheren Kodieren von links nach rechts */
        nachRechtsVerdrahtung = new int[verdrahtung.length];
        for(int i = 0; i < 26; i++) {
            nachRechtsVerdrahtung[i + verdrahtung[i]] =
                                0 - verdrahtung[i];
        }
    }
```

```
    public int kodieren(int position, boolean links) {
      return position;
    }

    public int nachLinksKodieren(int position) {
        return position;
    }

    public int nachRechtsKodieren(int position) {
        return position;
    }

    public void zaehlen() {
    }
}
```

D.2. Steckerbrett.java

```
package enigmasim;

public class Steckerbrett extends EnigmaModul {
/* Abgeleitet von EnigmaModul, reimplementiert die Methoden zum Kodieren */
    public Steckerbrett(EnigmaModul vorher,
                        EnigmaModul nachher,
                        int zaehler,
                        int[] verdrahtung) {
       super(vorher, nachher,  zaehler, verdrahtung);
    }

    public int kodieren(int position, boolean rechts) {
      if (rechts && vorher == null || nachher == null) {
          /* letztes Glied in der Kette, liefert das kodierte Zeichen */
          return nachRechtsKodieren(position);
      } else {
          nachher.zaehlen();
          /* Walzen weiterschalten */
          return nachher.kodieren(nachLinksKodieren(position), false);
          /* Kodieren des nachfolgenden Moduls aufrufen */
      }
    }
```

```
    public int nachLinksKodieren(int position) {
        /* Der Verdrahtung von rechts nach links folgen*/
        return position + verdrahtung[position];
    }

    public int nachRechtsKodieren(int position) {
        /* Der Verdrahtung von links nach rechts folgen*/
        return position + nachRechtsVerdrahtung[position];
    }
}
```

D.3. Walze.java

```
package enigmasim;

public class Walze extends EnigmaModul {
/* Abgeleitet von EnigmaModul, reimplementiert die Methoden zum Kodieren
       und Weiterschalten */
    public int ringstellung;

    public Walze(EnigmaModul vorher,
                 EnigmaModul nachher,
                 int zaehler,
                 int[] verdrahtung,
                 int ringstellung) {
       super(vorher, nachher, zaehler, verdrahtung);
       this.ringstellung = ringstellung;
    }

    public int kodieren(int position, boolean rechts) {
        if (rechts) {
            /* auf dem Rückweg durch die Walze */
            return vorher.kodieren(nachRechtsKodieren(position), true);
            /* Aufruf der Kodieren-Methode des Vorgängers */
        } else if (nachher == null) {
            /* Walze ist eine Umkehrwalze */
            return this.kodieren(nachLinksKodieren(position),
                                 nachher.nachher == null);
        } else {
            /* Auf dem Weg von rechts nach links durch die Walze */
            return nachher.kodieren(nachLinksKodieren(position),
                                    nachher.nachher == null);
```

```
            /* Aufruf der Kodieren-Methode des Nachfolgers */
        }
    }

    public int nachLinksKodieren(int position) {
        /* Der Verdrahtung von rechts nach links folgen. Dabei wird
           die aktuelle Stellung der Walze berücksichtigt */
        int Walzenstellung = (position + zaehler + ringstellung) % 26;
        return (position + verdrahtung[Walzenstellung] + 26) % 26;
    }

    public int nachRechtsKodieren(int position) {
        /* Der Verdrahtung von links nach rechts folgen. Dabei wird
           die aktuelle Stellung der Walze berücksichtigt */
        int Walzenstellung = (position + zaehler + ringstellung) % 26;
        return (position + nachRechtsVerdrahtung[Walzenstellung] + 26) % 26;
    }

    public void zaehlen() {
        /* Weiterschaltung der Walze */
        if (nachher != null) {
           /* Nur drehen, wenn es keine Umkehrwalze ist */
          zaehler++;
          zaehler = zaehler % 26;
           /* Zähler inkrementieren und normalisieren */
          if (zaehler == (verdrahtung[26] + ringstellung + 1) % 26) {
                /* Auf Position 26 der Verdrahtung ist die Nut zum
               Weiterschalten kodiert, ist diese erreicht, wird auch
               die nachfolgende Walze zum Drehen aufgefordert */
             nachher.zaehlen();
            }
        }
    }
}
```

D.4. Beispiel für die Verdrahtung einer Walze

Die Verdrahtungen der Walzen entsprechen denen der originalen Enigma. Sie werden in einem Array als relative Position zum besetzten Platz im Array hinterlegt. So bedeutet *wverdrahtung[6] = -3;*, dass der Buchstabe G mit dem Buchstaben D verdrahtet ist.

```
/* Walze I */
wverdrahtung[0] = 4;    wverdrahtung[1] = 9;    wverdrahtung[2] = 10;
```

```
wverdrahtung[3] = 2;    wverdrahtung[4] = 7;    wverdrahtung[5] = 1;
wverdrahtung[6] = -3;   wverdrahtung[7] = 9;    wverdrahtung[8] = 13;
wverdrahtung[9] = 16;   wverdrahtung[10] = 3;   wverdrahtung[11] = 8;
wverdrahtung[12] = 2;   wverdrahtung[13] = 9;   wverdrahtung[14] = 10;
wverdrahtung[15] = -8;  wverdrahtung[16] = 7;   wverdrahtung[17] = 3;
wverdrahtung[18] = 0;   wverdrahtung[19] = -4;  wverdrahtung[20] = -20;
wverdrahtung[21] = -13; wverdrahtung[22] = -21; wverdrahtung[23] = -6;
wverdrahtung[24] = -22; wverdrahtung[25] = -16; wverdrahtung[26] = 24;
```

Literaturverzeichnis

[1] Bauer, F. L. (1997). *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Berlin: Springer.

[2] Kruh, L. & Deavours, C. (2002). The Commercial Enigma – Beginnings of Machine Cryptography. *Cryptologia, Vol. XXVI* (1). [verfügbar unter http://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf]

[3] Singh, S. (2001). *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. München: dtv.