

Geschwister-Scholl-Gymnasium Velbert

Facharbeit Informatik

Die Enigma Verschlüsselung - woran sie gescheitert ist

Mattis Jung, Q1 25/26

09.01.2026 - 23.02.2026

6 Wochen

Inhaltsverzeichnis

1	Einleitung	2
2	Die Enigma - Maschine	2
2.1	Wie die Enigma - Maschine entstand	2
2.2	Wie die Enigma - Maschine funktioniert	2
2.2.1	Das Steckerbrett	2
2.2.2	Die Walzen	2
3	Die Schwächen der Enigma - Maschine	3
3.1	Die Umkehrwalze	3
3.2	Steckerbrett Bedingungen	3
3.3	Weitere Bedingungen	3
4	Meine Enigma Implementation	3
4.1	Wie funktioniert diese Implementation?	3
4.1.1	Die Enigma	3
4.1.2	Die Walze	4
5	Die perfekte Enigma - Maschine	4
5.1	Was ist anders an dieser Enigma - Maschine?	4
6	Fazit	4

1 Einleitung

2 Die Enigma - Maschine

Die Enigma - Maschine ist eine Chiffriermaschine, die durch die Nutzung von Permutation und Substitution der Buchstaben einer Nachricht, diese Buchstabe für Buchstabe verschlüsselt.

2.1 Wie die Enigma - Maschine entstand

Die Idee der Enigma - Maschine entstand bereits im ersten Weltkrieg, als die deutschen eine Möglichkeit brauchten geheime Nachrichten an die Front zu schicken, ohne dass Alliierte Truppen diese mitbekommen. Deshalb kam Arthur Scherbius (1878-1929) auf die Idee eine Rotor-Schlüsselmachine zu erfinden, welche er am 23. Februar 1918 auch patentieren ließ.¹ Der Name der Enigma - Maschine entstand Ende 1923, als Scherbius seine Erfindung nach dem Griechischem Wort *enigma* benannte, welches Rätsel bedeutet.

Über die Jahre wurde diese immer populärer in Deutschland und nach Ende des zweiten Weltkrieges wurde verschiedenste, von den deutschen zurückgelassene, Exemplare modifiziert und auch weiter benutzt. Ein Beispiel hierfür ist die *Norenigma*, welche eine in Norwegen modifizierte Version der deutschen Enigma - Maschine ist.

2.2 Wie die Enigma - Maschine funktioniert

Von Außen sieht die Enigma - Maschine einer Schreibmaschine nicht ganz unähnlich, nur hier hat man nicht nur die Tastatur, sondern auch ein Glühlampenbrett, wo es für jede Taste der Tastatur eine Glühlampe gibt, die aufleuchtet, wenn eine Taste gedrückt wird. Dazu besteht die Enigma - Maschine aus 2 wichtigen Chiffrierteilen.

2.2.1 Das Steckerbrett

Dort werden alle Buchstaben die es in der Tastatur gibt angezeigt und man kann Kabel in den jeweiligen Buchstaben stecken und diesen dann mit einem andern verbinden. Dies sorgt dafür, dass der eingegebene Buchstabe durch den zweiten ersetzt wird, also dass eine *Permutation* stattfindet. Wenn ein Buchstabe in der Enigma - Maschine mit einem anderen verkabelt ist, nennt man ihn *gesteckert*. In der Maschine sind immer 20 Buchstaben miteinander gesteckert und die restlichen 6 sind ungesteckert. Außerdem durften zwei im Alphabet aufeinanderfolgende Buchstaben nicht miteinander gesteckert sein. Diese beiden Regelungen machten die Entschlüsselung der Enigma - Maschine für die Alliierte nicht schwerer, sondern nur leichter.

2.2.2 Die Walzen

Diese haben auf beiden Seiten je 26 Kontaktpunkt, welche in der Walze mit je einem andern Kontaktpunkt verkabelt sind. Dies funktioniert aber nicht so, dass das A auf der rechten Seite immer mit dem A verkabelt ist, sondern meistens mit einem andern Buchstaben (E),

¹Patentschrift.

dadurch entsteht eine *Substitution*. Durch die Nutzung von meist 3 Walzen (Die *Enigma-M4* nutze beispielsweise 4) steigt die Verschlüsselungsstärke der Enigma-Maschine exponentiell. Die Walzen hatten außerdem eine oder mehrere Kerben, welche dafür sorgten, dass nicht nur die erste Walze rotiert, sondern auch die nächsten mit rotieren.

Da die meisten Walzen nur eine Kerbe hatten war es selten, dass sich die letzte Walze wirklich viel verändert. Für den Funkverkehr der Achsenmächte nach Japan hatten die Deutschen aber eine Alternative, da sie bei dieser Version der Enigma-Maschine nicht eine, sondern fünf Übertragungskerbene hatten, welche diese Enigma-Maschine stärker machte als die in Deutschland am meisten verbreiteten Enigma-Maschinen (*Enigma-T* oder auch *Tirpitz* genannte Enigma-Maschine für den Funk nach Japan). Aber auch in Deutschland gab es Enigma-Maschinen mit mehreren Übertragungskerbene, wie die Abwehr-Enigma (G), welche bis zu 17 Übertragungskerbene hatte.

3 Die Schwächen der Enigma-Maschine

Durch verschiedenste Regulierungen wurde die Enigma-Maschine nicht cryptisch gestärkt, sondern nur geschwächt.

3.1 Die Umkehrwalze

3.2 Steckerbrett Bedingungen

3.3 Weitere Bedingungen

Zudem gab es für jeden Monat eine Schlüsselkarte, auf welcher die Walzenlage, Ringstellung, Steckerverbindungen und Kenngruppen für den jeweiligen Tag standen. Diese durften nicht mit in Flugzeuge mitgenommen werden, da sie sonst einfacher in die Hände der Alliierten fallen konnten.

4 Meine Enigma Implementation

4.1 Wie funktioniert diese Implementation?

In dieser Version der Enigma-Maschine gibt es zwei verschiedene Klassen, welche miteinander interagieren und somit die eingegebene Nachricht verschlüsseln. Die erste und größere Klasse ist die Enigma-Klasse, in welcher die meiste Logik geschieht. Sie erstellt beim Starten des Verschlüsselns die Walzen, in welcher nur die einzelne Ersetzung der Buchstaben geschieht. Das Steckerbrett ist Teil der Enigma-Klasse und tauscht die gesteckerten Buchstaben vor und nach durchlaufen der Rotoren mit dem jeweils anderen aus.

4.1.1 Die Enigma

Die Klasse Enigma wird mit folgenden Parametern initialisiert und sieht so aus:

Parameter:

self: Wird benötigt, damit Objekte dieser Klasse auf sich selbst zurückverweisen können. Parameter in allen Funktionen der Klasse.

name (str): Name der Enigma - Maschine, bestehend aus *Enigma* und der Modellnummer *I*, welches mit einem - getrennt ist. Dient zur identifizierung der Art der Enigma - Maschine. (*Enigma - I*, *Enigma - M3*, *Enigma - G*, etc.)

vorlage (dict): Dictionary, welches alle wichtigen Informationen für die Walzenlage, Ringstellung, Steckerverbindung und Kenngruppe beinhaltet. Die Walzenlage ist eine Liste an Strings, welche die jeweiligen Walzen spezifizieren. Die Ringstellung ist eine Liste an Zahlen, welche den „Rotationsversatz zwischen der inneren Verdrahtung der Walzen und den außen zu sehenden Buchstaben oder Zahlen“² angeben. Die Steckerverbindung ist eine 10 Elemente lange Liste and 2 Zeichen langen Strings, welche angibt, welche Buchstaben miteinander gesteckt sind, da es nur 10 Elemente gibt müssen 6 Buchstaben des Alphabets ungesteckt sein. Die Kenngruppen ist eine Liste an Strings, welche mögliche Kenngruppen für den jeweiligen Tag angeben. Davon müssen drei in die zu verschlüsselne Nachricht eingebaut werden, inden man sie permutiert mit zwei Füllbuchstaben der Nachricht unverschlüsselt voranstellt.

startingPosition (str): Ein String bestehend aus drei Zeichen, welche die Grundstellung für die Walzen angibt. Das erste Zeichen steht für die schnellste Walze (ganz rechts), das zweite für die mittlere Walze und das dritte für die langsamste Walze (ganz links). Dieser wird beim initialisieren in eine Liste mit dem jeweiligen Zahlenwert für den Buchstaben umgewandelt.

Funktionen:

encode:

getEnigmaString:

stecker:

steckerbrett:

rotors:

rotate:

findRotors:

4.1.2 Die Walze

Die Klasse Walze wird mit folgenden Parametern initialisiert und sieht so aus:

5 Die perfekte Enigma - Maschine

5.1 Was ist anders an dieser Enigma - Maschine?

6 Fazit

²dewiki:Enigma.