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

0.1 Einleitung

0.2 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.

0.2.1 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-Schlüsselmaschine zu erfinden, welche er am 23. Februar 1918 auch patentieren ließ. [2] Der Name der Enigma - Maschine entstand Ende 1923, als Scherbius seine Erfindung nach dem Griechischem Wort *enigma* bennante, 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.

0.2.2 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:

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. 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), 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 letzt Walze wirklich viel verändert. Für den Funkverkehr der Achsenmächte nach Japan hatten die deut-

schen aber eine alternative, da sie bei dieser Version der Enigma - Maschine nicht eine, sondern fünf Übertragungskerben 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 [1]). Aber auch in Deutschland gab es Enigma - Maschine mit mehreren Übertragungskerben, wie die Abwehr - Enigma (G), welche bis zu 17 Übertragungskerben hatte.

0.3 Was sind die Schwächen der Enigma - Maschine

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

0.4 Meine Enigma Implementation

0.4.1 Wie funktioniert diese Implementation?

0.5 Die perfekte Enigma - Maschine

0.5.1 Was ist anders an dieser Enigma - Maschine?

Literatur

[1] *Enigma-T*. URL: https://de.wikipedia.org/wiki/Enigma-T (besucht am 07. 02. 2026).

[2] *Patentschrift Chiffrierapparat DRP Nr. 416 219*. URL: https://www.cdvandt.org/Enigma%20DE416219C1.pdf (besucht am 06. 02. 2026).