

**Ein praktischer Ansatz zur Dechiffrierung von Texten der
Enigma-Maschine**

Kryptoanalyse der Enigma-Maschine

Emanuel Schäffer

11. September 2024

RWU–University of Applied Sciences

Enigma-Nachrichten können dechiffriert werden, wenn die Rotorauswahl¹, die Rotor-, Ringstellungen und die Steckereinstellungen einzeln wiederhergestellt werden. Die Wiederherstellung der Nachrichtenschlüsselleinstellung ist empfindlich genug, um die korrekte Rotorreihenfolge zu unterscheiden. Die Methode wird an einer 647 Zeichen langen Nachricht demonstriert und ihre Leistung für unterschiedliche Nachrichtenlängen und verwendete Steckeranzahlen geschätzt.

¹Hier wird im Allgemeinen nur die Enigma M1 mit 5 Walzen betrachtet.

1 Enigma

Die Enigma ist eine Rotor-Chiffriermaschine, welche hauptsächlich im 2. Weltkrieg Einsatz fand. Die von der Wehrmacht modifizierte Enigma verfügte zuerst über drei Walzen mit zusätzlich einem Reflektor. Jeder dieser Walzen führte eine monoalphabetische Substitution durch. Die rechte Walze wurde bei jedem Tastendruck eine Position weiter gerückt. Hat diese Walze eine komplette Rotation geleistet, rückte die Walze links neben ihr eine Position weiter¹. Neuerungen waren das Steckerbrett (siehe Abb. 1.1) und gegen Ende des Krieges wurden Enigmen mit bis zu vier Walzen eingesetzt. Ich werde mich des weiteren, wenn nicht ausdrücklich erwähnt auf die Enigma M3 mit drei Walzen beziehen.

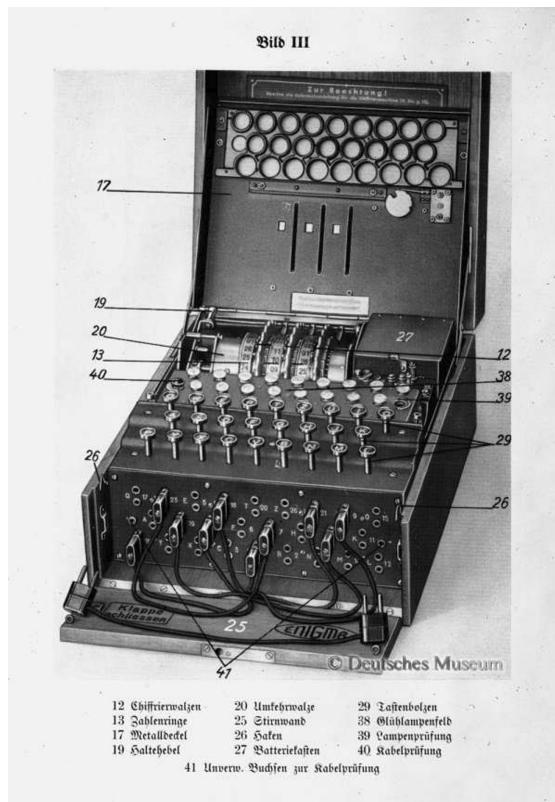


Abbildung 1.1: Die Enigma Maschine

¹Eine Analogie hierfür ist der Kilometerzähler eines mechanischen Tachometers oder das Verhalten von Sekunden, Minuten und Stundenzeiger einer Uhr.

Bei der Enigma wurde jeden Tag eine Tagesschlüssel eingestellt, welcher durch ein Code-Buch vorgegeben war. Dieser Tagesschlüssel bestand daraus, welche drei der fünf Walzen der Schlüssler in welcher Reihenfolge einzusetzen hat. Ferner musste er die Walzenstellung einstellen. Sie bestimmt die Ausgangsstellung der Walzen. Diese konnte durch ein Sichtfenster erblickt werden.

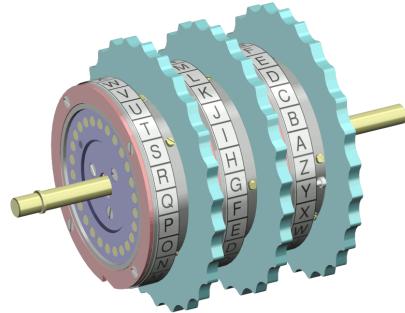


Abbildung 1.2: Enigma-Walzen

Zusätzlich musste der Schlüssler die Ringstellung des Tages einstellen. Die Ringstellung veränderte die Relation der Buchstaben und der internen Verdrahtung und bewegte die Übertragskerbe. Siehe Abb. 1.3

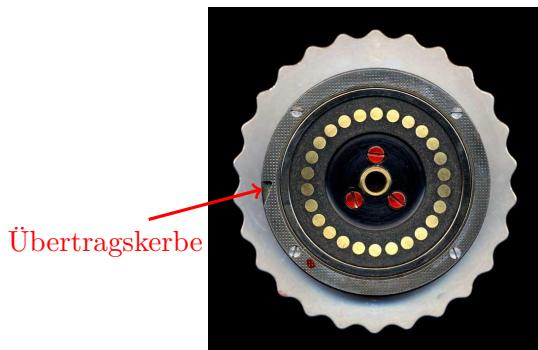


Abbildung 1.3: Walzen Frontansicht mit Übertragskerbe

2 Häufigkeitsanalyse

2.1 Koinzidenzindex

Zunächst benötigen wir ein geeignetes Maß, um den Grad der Annäherung eines teilweise dechiffrierten Klartextes an authentisches Deutsch abzuschätzen. Dafür verwenden wir den Koinzidenzindex:

$$IC = \frac{\sum_{i=A}^Z f_i(f_i - 1)}{N(N - 1)}$$

Sei f_i die Häufigkeit des Buchstabens in Abhängigkeit von i und N die Gesamtanzahl der Buchstaben. Wir Summieren also die Anzahl der Buchstabenpaare auf, und teilen diese durch die Anzahl der allgemein möglichen Buchstabenpaare. Der Koinzidenzindex ist also ein Maß für die Buchstabenverteilung. Für ein Text bestehend aus zufälligen Buchstaben beträgt der $IC \approx 0.038$; wobei er für Deutsch ≈ 0.076 beträgt.

Bemerkungen:

Improvements:

Base: 8.5s

Nur letzte Buchstaben testen: 3.6s

IC: 3.3s

Low Level IO: 3.31s

Nur erster char testen an der Position, an dem das Schlagwort stehen muss: 2.25s

3 Quellen