Geschwister-Scholl-Gymnasium Velbert

Die Enigmaverschlüsselung - Woran sie gescheitert ist

Mattis Jung

21. Februar 2026

Dies ist ein kleiner Wegweiser für das Schreiben einer Facharbeit. Der Schwerpunkt liegt hier auf der Verwendung von LaTeX.

Am einfachsten ist es vermutlich, dieses Dokument als PDF anzuschauen und nebenbei im Quelltext nachzuschauen, wie dies und das umgesetzt wurde. Parallel dazu füllt man sein eigenes Dokument (*Facharbeit.tex*).

Inhaltsverzeichnis

1 Einleitung

2 Die Enigma

Die Enigma ist eine elektromechanische Chiffriermaschine. Sie verschlüsselt eine Nachricht buchstabenweise, indem sie die Zeichen über mehrere Stufen vertauscht (*Permutation*) und ersetzt (*Substitution*).

2.1 Wie sie entstand

Die Idee zur Enigma entstand bereits im Ersten Weltkrieg: Die Deutschen benötigten eine Möglichkeit, geheime Nachrichten an die Front zu übermitteln, ohne dass alliierte Truppen sie mitlesen konnten. Arthur Scherbius (1878 - 1929) entwickelte deshalb die Idee einer Rotor - Schlüsselmaschine und ließ sie am 23. Februar 1918 patentieren. [3] Ende 1923 erhielt die Maschine ihren Namen, als Scherbius die Erfindung nach dem griechischen Wort *enigma* („Rätsel“) benannte.

Mit der Zeit wurde die Enigma in Deutschland immer populärer. Nach dem Ende des Zweiten Weltkriegs wurden viele von den Deutschen zurückgelassene Exemplare umgebaut und weiterverwendet. Ein Beispiel ist die *Norenigma*, eine in Norwegen modifizierte Version der deutschen Enigma.

2.2 Wie sie funktioniert

Von außen erinnert die Enigma an eine Schreibmaschine. Neben der Tastatur besitzt sie jedoch ein Glühlampenfeld: Zu jeder Taste gehört eine Lampe, die beim Tastendruck den verschlüsselten Buchstaben anzeigt. Im Kern arbeitet die Enigma mit zwei entscheidenden Chiffrierelementen: dem Steckerbrett und den Walzen.

2.2.1 Das Steckerbrett

Auf dem Steckerbrett sind alle Buchstaben der Tastatur aufgeführt. Mit Steckerkabeln lassen sich jeweils zwei Buchstaben miteinander verbinden. Dadurch wird ein eingegebener Buchstabe in seinen Partnerbuchstaben umgewandelt. Es entsteht eine zusätzliche Vertauschung (*Permutation*).

Ist ein Buchstabe mit einem anderen verbunden, nennt man ihn *gesteckert*. In der Standardkonfiguration werden 10 Kabel gesteckt: 20 Buchstaben sind paarweise verbunden, die übrigen 6 bleiben ungesteckert. Zusätzlich galt die Regel, dass zwei im Alphabet direkt aufeinanderfolgende Buchstaben nicht miteinander gesteckert werden durften. Solche Vorgaben machten die Arbeit der Alliierten nicht schwieriger, sondern schränkten die möglichen Einstellungen weiter ein.

2.2.2 Die Walzen

Die Walzen besitzen auf beiden Seiten jeweils 26 Kontaktpunkte. Im Inneren ist jeder Kontaktpunkt mit genau einem anderen verdrahtet. Das bedeutet: Ein A wird nicht zwangsläufig wieder zu A, sondern beispielsweise zu E, eine *Substitution*. Werden mehrere Walzen hintereinandergeschaltet (meist drei; die *Enigma - M4* nutzte beispielsweise vier), wächst die Anzahl der möglichen Verschlüsselungen sprunghaft. Außerdem drehen sich die Walzen weiter: Nach jedem Tastendruck rotiert mindestens die rechte Walze. Erreicht sie ihre Kerbe, wird auch die nächste Walze weitergeschaltet usw.

Da die meisten Walzen nur eine Kerbe besaßen, änderte sich die linke Walze im Vergleich selten. Für den Funkverkehr der Achsenmächte nach Japan verwendeten die Deutschen jedoch eine Variante mit fünf Übertragungskerben, was diese Version gegenüber den in Deutschland am weitesten verbreiteten Enigma - Modellen stärkte (*Enigma - T*, auch *Tirpitz* genannt). Aber auch in Deutschland gab es Enigma - Varianten mit mehreren Übertragungskerben, wie die Abwehr - Enigma (G), die bis zu 17 Übert ragungskerben hatte.

3 Die Schwächen der Enigma

Durch verschiedene Regulierungen wurde die Enigma nicht kryptografisch gestärkt, sondern in entscheidenden Punkten sogar geschwächt.

Die Umkehrwalze funktioniert nicht so wie die anderen Walzen, da sie nur eine Kontaktplatte hat, auf welcher die Kontakte miteinander verkabelt ist. Das führt dazu, dass wenn man ein B eintippt und ein K aufleuchtet, auch beim eintippen vom K das B aufleuchtet.

3.1 Steckerbrett Bedingungen

Das Steckerbrett vertauscht Buchstaben, die miteinander gesteckert sind. Dabei durften aber nur 20 von den 26 Buchstaben gesteckert sein. Die restlichen sechs blieben ungesteckert.

3.2 Weitere Bedingungen

Zudem gab es für jeden Monat eine Schlüsseltafel, auf der Walzenlage, Ringstellung, Steckerverbindungen und Kenngruppen für jeden Tag festgelegt waren. Diese Tafeln durften nicht an Bord von Flugzeugen mitgenommen werden, da sie sonst leichter in die Hände der Alliierten fallen konnten.

4 Meine Enigma Implementierung

4.1 Wie funktioniert diese Implementierung?

In meiner Version der Enigma arbeiten zwei Klassen zusammen, um eine eingegebene Nachricht zu verschlüsseln. Die größere Klasse ist die Enigma - Klasse: Dort liegt die zentrale Logik. Beim Start der Verschlüsselung erzeugt sie die benötigten Walzen; in diesen findet die eigentliche Buchstaben - Ersetzung statt. Das Steckerbrett ist ebenfalls Teil der Enigma - Klasse und vertauscht gesteckerte Buchstaben sowohl vor als auch nach dem Durchlaufen der Rotoren.

4.1.1 Die Enigma

Die Klasse Enigma wird mit folgenden Parametern initialisiert und ist wie folgt aufgebaut:

Parameter:

name (str): Name der Enigma, bestehend aus *Enigma* und der Modellbezeichnung (z. B. *I*), getrennt durch ein -. Dient zur Identifizierung der Art der Enigma (*Enigma - I, Enigma - M3, Enigma - G*, etc.).

vorlage (dict): Dictionary, das alle wichtigen Informationen zu Walzenlage, Ringstellung, Steckerverbindungen und Kenngruppen enthält. Die Walzenlage ist eine Liste von Strings, die die jeweiligen Walzen spezifizieren. Die Ringstellung ist eine Liste von Zahlen, die den Rotationsversatz zwischen der inneren Verdrahtung der Walzen und den außen sichtbaren Buchstaben bzw. Zahlen angibt. Die Steckerverbindung ist eine zehn Elemente lange Liste aus Strings mit je zwei Zeichen. Sie legt fest, welche Buchstaben miteinander gesteckert sind; dadurch bleiben sechs Buchstaben des Alphabets ungesteckert. Die Kenngruppen sind eine Liste von Strings, die mögliche Kenngruppen für den jeweiligen Tag angeben. Davon müssen drei in die zu verschlüsselnde Nachricht eingebaut werden, indem man sie permutiert und mit zwei Füllbuchstaben unverschlüsselt voranstellt.

startingPosition (str): Ein String aus drei Zeichen, der die Grundstellung der Walzen festlegt. 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). Beim Initialisieren wird dieser String in eine Liste mit den jeweiligen Zahlenwerten der Buchstaben umgewandelt.

Funktionen:

encode: Verschlüsselt den eingegebenen Text.

getEnigmaString: Formatiert den Ausgabetext (z. B. in 5er - Gruppen).

stecker: Wendet eine einzelne Stecker - Vertauschung an.

steckerbrett: Wendet das Steckerbrett auf einen gesamten Text an.

rotors: Führt den Lauf durch die Rotoren aus.

rotate: Rotiert die Walzen gemäß Kerben - Mechanik.
findRotors: Lädt und erzeugt die benötigten Walzen.

4.1.2 Die Walze

Die Klasse Walze wird mit folgenden Parametern initialisiert und ist entsprechend aufgebaut:

5 Die perfekte Enigma

5.1 Was ist anders an dieser Enigma?

6 Fazit

7 Einleitung

> Das Lernen macht stets dann Verdruß', wenn man's nicht will, es aber muss.
>
> Heinz Erhardt (1909 - 1979)

8 Ein bißchen zu LaTeX und zur Typographie

8.1 Typographische Feinheiten, die viele nicht kennen...

Hier mal der Unterscheid zwischen einem ganzen und einem halben[3] (richtige Version) Leerzeichen vor Einheiten:
100 m oder auch 100m sehen weniger schön aus, als 100 m. Ein Eurosymbol erzeugt man durch einen Befehl (siehe Quelltext): 22 €... Gleiches gilt für ein Prozentzeichen %, was ja eigentlich den Text im Quelltext auskommentieren würde... Bei Abkürzungen kommt ebenfalls das halbe Leerzeichen zur Anwendung. Man schreibt z. B. (nicht z.B. oder z. B.) 70 % statt 70% oder gar 70 % (halbes Leerzeichen). Siehe Quelltext.

Um etwas wichtiges hervorzuheben, verwendet man übrigens nicht den aufdringlichen (wenn auch leider von vielen verwendeten) **Fettdruck** sondern die dezente *italienische* Variante! Benötigt man mehr, gibt es auch noch: etwas ohne Serifen (gesehen?) oder `Schreibmaschinenschrift`. Natürlich geht noch viel mehr allerdings sollte man es vermeiden Schriftarten zu mischen, wenn man nicht ganz genau weiß was man tut. Die italienische Variante reicht in der Regel.

Absätze sind am Anfang immer etwas eingerückt und werden im Quelltext durch eine Leerzeile erzeugt.

Sehr empfehlenswert ist auch die kleine PDF „typokurz[1]".

8.2 Ein paar Beispiele für den Einsatz von LaTeX

LaTeX, ausgesprochen „Latech" funktioniert nach dem Prinzip des Textsatzes, Word und andere nach dem Wortsatzverfahren.

Word funktioniert nach dem Prinzip: „What You See Is What You Get" (WYSIWIG) - das fertige Ergebnis ist von Anfang an auf dem PC-Bildschirm zu erkennen. Die LaTeX-Community setzt diesem Slogan ihr eigenes Motto entgegen: WYGIWYM steht für „What You Get Is What You Mean" - Man bekommt das, was man auch wirklich beabsichtigt hat.

8.2.1 Darstellung Chemie

$\mathrm{Po} - - - {}^{56}\mathrm{Fe} - - - {}^{13}_{6}\mathrm{C}$

$\mathrm{n} + \mathrm{H} \rightarrow \mathrm{D} + \gamma(2.2\,\mathrm{MeV})$

${}^{13}_{6}\mathrm{C} + \alpha(5.314\,\mathrm{MeV}) \rightarrow {}^{16}\mathrm{O}^{**} + n$

8.2.2 Darstellung Mathematik

$$\int_0^6 x^2 dx = 72 \tag{1}$$

Umgebungen, wie hier die *align*-Umgebung können zusätzlich mit einem Sternchen versehen werden, wie beispielsweise im nächsten Fall, wodurch die Formelnummerierung (auf die übrigens wieder referenziert werden können) ausgeschaltet werden kann.

Hier werden mehrere Formeln untereinander am Gleichheitszeichen ausgerichtet dargestellt.

$$\begin{aligned} \int_0^6 x^2 dx &= 72 \\ f(x) &= e^{\pi \cdot t} \\ \vec{x} &= \begin{pmatrix} 2 \\ 3 \\ -4 \end{pmatrix} \\ A &= \begin{pmatrix} 2 & 3 \\ -4 & 2 \\ 3 & -4 \end{pmatrix} \end{aligned}$$

Oder mal 'ne Polynomdivision:

$$\begin{array}{rrrrl} \big(& x^4 - 7x^3 & + 3x & - 2 \big) : \big(x - 2\big) = x^3 - 5x^2 - 10x - 17 + \dfrac{-36}{x-2} \\ & \underline{- x^4 + 2x^3} & & & \\ & - 5x^3 & & & \\ & \underline{5x^3 - 10x^2} & & & \\ & - 10x^2 & + 3x & & \\ & \underline{10x^2 - 20x} & & & \\ & - 17x & - 2 & & \\ & \underline{17x - 34} & & & \\ & - 36 & & & \end{array}$$

8.2.3 Darstellung von Quellcode

```
class Fahrzeug{
    String hersteller;
    String farbe;

    //--- Konstruktor, initialisiert die Datenfelder
    Fahrzeug(String derHersteller, String dieFarbe){
        hersteller = derHersteller;
        farbe = dieFarbe;
    }

    //--- Methoden des Fahrzeugs
    beschleunigen(){

    }

    bremsen(){

    }

    links(){

    }

    rechts(){

    }
}
```

8.2.4 Darstellung von Zitaten, Quellen, etc.

Der folgende Zitierstil[2] wird unter anderem in der weltbekannten Zeitschrift *nature* verwendet. Die Quellen werden numerisch automatisch in der erwähnten Reihenfolge im Literaturverzeichnis gelistet.

In LaTeX lassen sich über *Syle-Vorgaben* auch andere Zitierstile umsetzen, hier gibt es genügend Möglichkeiten für Mediziner, Geisteswissenschaftler oder Juristen. Da muß man möglicherweise etwas recherchieren.

8.2.5 Die Datei *literatur.bib*

In der Datei befinden sich letztlich alle Quellen. Dazu werden diese einfach nach einem festgelegten Schema festgehalten und LaTeX erstellt daraus das Literaturverzeichnis (siehe Ende des Dokuments). Der Aufbau ist im Prinzip wie folgt:

Am Besten gleich mal mit dem Literaturverzeichnis vergleichen (in normalem Editor öffnen)!

8.2.6 Zitate aus anderen Werken

Man kann in einer wissenschaftlichen Arbeit durchaus per „Copy & Paste“ einen Text übernehmen. Dieser muß dann allerdings mit Angabe der Quelle als Zitat (z. B. beidseitig eingerückt) dargestellt werden.

> Beispiel für ein Zitat (quote). Es gibt aber auch (quotation) für längere Zitate oder sogar (verse) für Verse... Man erkennt hier die beidseitige Einrückung.

8.2.7 Gedichte in Versform

Wie wäre es mit Gedichten?

> Ein jeder Stier hat oben vorn
> auf jeder Seite je ein Horn;
> doch ist es ihm nicht zuzumuten,
> auf so 'nem Horn auch noch zu tuten.
> Nicht drum, weil er nicht tuten kann,
> nein, er kommt mit dem Maul nicht 'ran!.

8.2.8 Farbhervorhebungen

Texte lassen sich natürlich auch einfärben, das kann z. B. bei der Beschreibung von Batterieanschlüssen hilfreich sein: Plus ... Minus.

8.2.9 Bilder

Bilder, Tabellen, etc. werden in der Regel in einer *figure-Umgebung* gesetzt. Diese ermöglicht einem beispielsweise auch den Verweis (siehe Abb.: 1, siehe auch Quelltext!) auf ein Bild im laufenden Text.

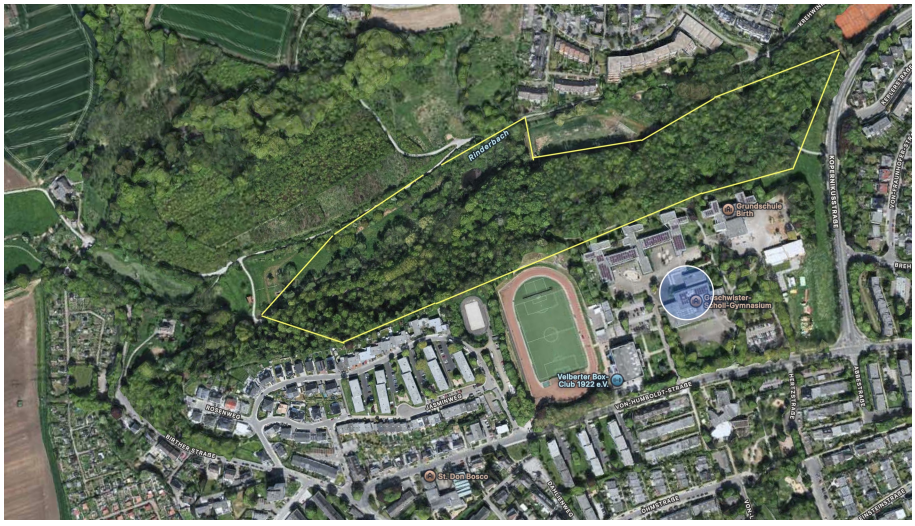

Abbildung 1: Satellitenaufnahme der Untersuchungsfläche

Name	Vorname	Alter	Geburtstag	Geburtsort
Katrin	Lollipop	16	1.1.1999	Velbert
Uschi	Lomboku	17	1.1.1998	Essen
Pauline	Fümmli	17	12.5.1999	Zürich

8.2.10 Tabellen

8.2.11 Erweiterungen

Es gibt für LaTeX wirklich alles Mögliche in Form von Zusatzpaketen, die am Anfang des Dokuments mit dem Befehl \usepackage{...} importiert werden können. Es gibt z. B. Pakete für Kochbücher, Puzzle, Kreuzworträtsel, elektronische Schaltsymbole und weiß der Geier was noch.

8.3 Vorbereitungen zum Schreiben einer Facharbeit

Während der Orientierungsphase ist es sehr wichtig, sich Notizen zu machen. Jede gesammelte Information sollte in Stichworten festgehalten werden und zwar so, daß sie jederzeit wiedergefunden werden kann. In einer PDF aus dem Internet habe ich beispielsweise Informationen zur Typographie entdeckt, die mir ganz interessant erschienen. Also erstelle ich mir eine entsprechende Notiz mit Informationen, die später evtl. nützlich sein könnten. Ich weiß ja jetzt noch nicht, ob ich davon etwas verwenden möchte und dies am Ende in den Quellen anzugeben gedenke.

Meine ersten Notizen könnten also etwa so aussehen:

Notizen

PDF-Datei: Christoph Bier - „typokurz – Einige wichtige typografische Regeln“ - Könnte für später ganz interessant sein
(Datei: /home/Facharbeit/PDFs/ typokurz.pdf); Autor: Christoph Bier, weitere Infos im PDF

Internetseite: https://www.overleaf.com ... Ein Onlineeditor. Vielleicht irgendwo erwähnen für Leute, die LaTeX nicht installieren können?

Nach und nach taucht man immer tiefer in das Thema ein und nach einiger Zeit kann man über viele Aspekte bereits frei reden und hat Zusammenhänge verstanden. Dinge, die anfangs wichtig erschienen wurden zwischenzeitlich verworfen, dafür kamen neue, andere Aspekte hinzu.

20 %

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Facharbeit selbstständig angefertigt, keine anderen als die angegebenen Hilfsmittel benutzt und die Stellen der Facharbeit, die im Wortlaut oder im wesentlichen Inhalt von anderen Autoren übernommen wurden, mit genauer Quellenangabe kenntlich gemacht habe.

Velbert, den 21. Februar 2026

Vorname Nachname

Literatur

[1] Christoph Bier. *typokurz - Einige wichtige typografische Regeln*. - Onlineresource, eingesehen am 30.09.2025. 2008. URL: `https://zvisionwelt.wordpress.com/wp-content/uploads/2012/01/typokurz.pdf`.

[2] Max Mustermann und Uschi Müller. *Das Leben der Eintagsfliege*. 5., vollständig überarbeitete Auflage. Stuttgart: Klimmbimm Verlag, 2008.

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