Informatik

**Lennart Schrader, 70476901**

**Till Hajek, 70476901**

Weitere Programmiersprache  
Dokumentation Implementierung einer Enigma-Rotorschlüsselmaschine

Ostfalia Hochschule für angewandte Wissenschaften

– Hochschule Wolfenbüttel

Erste/-r Prüfer/-in: Prof. Dr. Hans Grönniger

Eingereicht am 06.06.2021

Inhalt

[1 Einführung 2](#_Toc73304282)

# Einleitung

Die Enigma-Rotorschlüsselmaschine wurde bereits 1918 vom deutschen Elektroingenieur Arthur Scherbius erfunden[[1]](#footnote-1). Ihre große Bekanntheit erlangt die Enigma jedoch durch die Verwendung zur Verschlüsselung Nachrichtenverkehr und Funksprüchen des deutschen Militärs, der Wehrmacht, in der Zeit des Nationalsozialismus. Neben der Wehrmacht nutzten auch die Polizei, sowie Geheimdienste und andere Institutionen des dritten Reiches verschiedene Modelle der Enigma.   
Bis zum Ende des zweiten Weltkrieges wurden schätzungsweise ~40.000 Enigma-Maschinen ausgeliefert[[2]](#footnote-2).  
Obwohl Enigma-Nachrichten erstmals im Januar 1940 durch das britische Kryptologenteam in Bletchley Park um Alan Turing herum entschlüsselt wurden[[3]](#footnote-3), kamen Variationen der Enigma dennoch im Koreakrieg 1965 zum Einsatz[[4]](#footnote-4).  
Die Verschlüsselung durch die Enigma erfolgt Zeichen für Zeichen, mögliche Eingaben sind lediglich die 26 Buchstaben des lateinischen Alphabets. Die Eingabe eines Buchstabens auf der Tastatur löst ein elektrisches Signal aus, welches an die erste bewegliche Walze weitergeleitet wird. Diese Walze hat für jeden Buchstaben einen entsprechenden Kontakt auf der eingehenden Seite, weitergeleitet wird jedoch ein anderer Buchstabe. In einer Enigma sind typischer Weise drei solcher Walzen verbaut. Die erste Walze dreht sich um eine Position weiter. Wurde die erste Walze vollständig rotiert, so wird die nächste Walze um eine Position gedreht, das Gleiche gilt für die zweite und dritte Walze. Somit haben zwei identische Eingaben eine sich unterscheidende Verschlüsselung.  
Nachdem eine Eingabe dreimal substituiert wurde wird Diese einmalig „statisch“ verschlüsselt und, in umgedrehter Reihenfolge, durch die drei Walzen gesendet.  
Die endgültige Verschlüsselung wird dem Benutzer in Form von aufleuchtenden Lampen mit entsprechen Buchstaben angezeigt. Eine zusätzliche Maßnahme zur Erhöhung der Sicherheit ist die Verwendung eines sogenannten „Steckbrettes“, durch welches die Ein- und Ausgaben initial bzw. final verschlüsselt werden. Hierbei handelt es sich um ein simples Umleiten der Signale durch das Stecken eines Kabels.   
Der Schlüssel für die Verschlüsselung und Entschlüsselung der Nachrichten ist beim Verwenden einer Enigma gleich, es handelt sich demnach um eine symmetrische Verschlüsselung. Dieser ergibt sich aus der Verwendung, Reihenfolge und Stellung der Walzen, der statischen Verschlüsselung nach und vor der Walzensubstitution und der genutzten Steckverbindungen.

## Motivation

Im Rahmen der Lehrveranstaltung “Weitere Programmiersprache SoSe 2021“ haben wir, Lennart Schrader und Till Hajek, uns dafür entschieden, eine Simulation einer in Kaptiel 1 beschriebenen Enigmaverschlüsselungsmaschine in der Programmiersprache Haskell zu implementieren.   
Die Aufgabenstellung durfte selbst gewählt werden, jedoch sollte auf die Implementierung einer GUI verzichtet werden. Wir beide waren fanden das Thema Verschlüsselung sehr interessant und sind dadurch auf die Idee gekommen eine Verschlüsselungsmaschine nachzubauen. Da Haskell eine funktionale Programmiersprache ist, waren wir davon überzeugt, Haskell würde sich gut für eine solche Implementierung eignen.

## Kurzbeschreibung

Unser Programm simuliert die Verschlüsselung einer Nachricht durch eine Enigma. Wie genau diese Verschlüsselung erfolgt ist in Kapitel 1 beschrieben und kann für besseres Verständnis auch der Abbildung 1 aus dem Anhang entnommen werden. Eine grafische Nutzeroberfläche ist nicht implementiert, die Ausführung des Programms erfolgt über die Kommandozeile.

# Erläuterungen zur Implementierung

Die Implementierung ist in zwei Modules zu unterteilen: **components.hs** und **interface.hs.**  
In components.hs werden die einzelnen Bestand- bzw. Bauteile der Enigma definiert, Funktionen, welche die Mechanismen einer Enigma-Maschine abbilden sollen, sowie die letztendliche Verschlüsselung sind ebenso enthalten. Das interface.hs Module importiert die benötigten Bauteile und wenige zusammengesetzte Funktionen aus components.hs. Weiter beinhaltet das Interface neben der Main-Funktion auch Definitionen, sowie Funktionen, welche für die Überprüfung der Benutzereingaben nötig sind.

## components.hs

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

## interface.hs

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

# Überlegung zu einer möglichen Implementierung in Python

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

# Fazit

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

# Anhang

Chart

Description automatically generated with low confidence

Abbildung https://www.mpoweruk.com/enigma.htm Enigma Encipherment Stages [abgerufen 30.05.2021, 23:20]

01.04. Einreichung von Vorschlägen

20-30h aufwand

5-6 Seiten ausarbeitung + code

Gliederung:

Einleitung/ Motivation/ Kurzbeschreibung 1 Seite

Erläuterung zur Implementierung 3 Seiten

Überlegung zur phyton Umsetzung 1 Seite

Schluss/ Fazit 0.5 Seiten

1. https://www.mpoweruk.com/enigma.htm [abgerufen 30.05.2021, 23:20] [↑](#footnote-ref-1)
2. https://cryptocellar.org/enigma/e-history/konski&krueger-production.pdf [abgerufen 30.05.2021, 23:20] [↑](#footnote-ref-2)
3. https://www.wissen.de/wie-der-code-der-legendaeren-enigma-maschine-geknackt-wurde [abgerufen 30.05.2021, 23:20] [↑](#footnote-ref-3)
4. https://web.archive.org/web/20160825110549/http://scienceblogs.de/klausis-krypto-kolumne/files/2016/08/Koreafunk-1964\_65-Chiffrierdienst.pdf [abgerufen 30.05.2021, 23:20] [↑](#footnote-ref-4)