



Enigma Simulator Bedienungsanleitung

Jasley Jangk

Inhaltsverzeichnis

1. Einführung	3
2. Erklärung der Grafischen Benutzeroberfläche	3
3. Erklärung der Bedienelemente	5
3.1. Walzen Auswahl 7. - 10.	5
3.2. Umkehrwalze 6.	5
3.3. Walzenstellung 11. – 14.	5
3.4. Ringstellung 15. – 18.	5
3.5. Steckbrett 27.	5
3.6. Umschalter Enigma M4 / M3 19.	5
3.7. Schnellspeichern / Schnellladen 20.	5
3.8. Zurücksetzen 23.	5
3.9. Einstellungen setzen 24.	5
3.10. Zufällige Einstellungen Erzeugen 22.	6
4. Erklärung der Einstellungen	6
5. Erklärung des Key Manager Systems (Einstellungen zu Schlüssel)	7
6. Laden und Speichern von Einstellungen	7
7. Erklärung des Original Enigma Mode	7
8. Erklärung Analysemonitor	8
9. Beispiel für eine Verschlüsselung / Vorgehen bei einer Ver- oder Entschlüsselung	10
Beispiel Text zum Entschlüsseln	11
10. Informationen Zur Installation	12
11. Weitere Informationen	12
12. Lizenz (CC-BY-4.0)	12

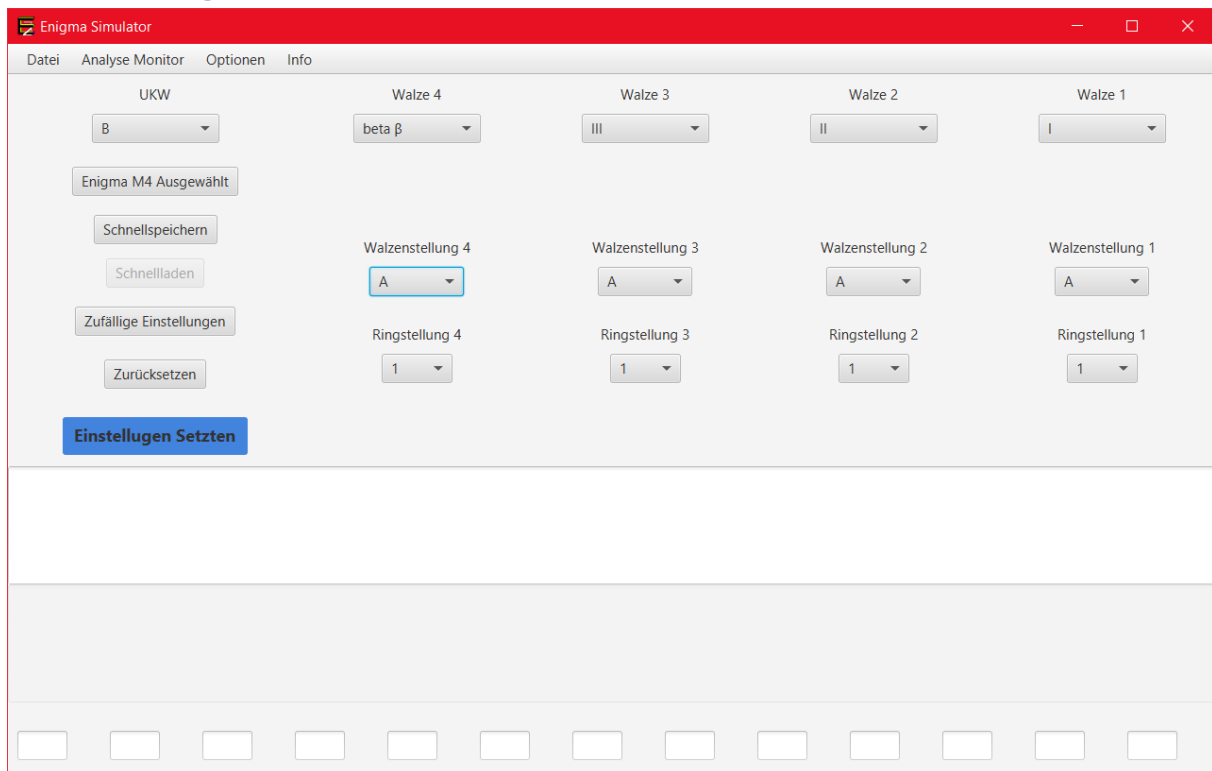
1. Einführung

Der Enigma Simulator ist eine Anwendung der einem genauem Nachbau in Software einer Enigma Verschlüsselungsmaschine der Version M3 und M4 aus den Jahren 1934 bis 1945 entspricht. Mit dieser Anwendung lassen sich Texte ver- und entschlüsseln um diese sicher seinem Gegenüber zukommen zu lassen. Die Verschlüsselungstechnik ist zwar gebrochen jedoch immer noch sehr eindrucksvoll.

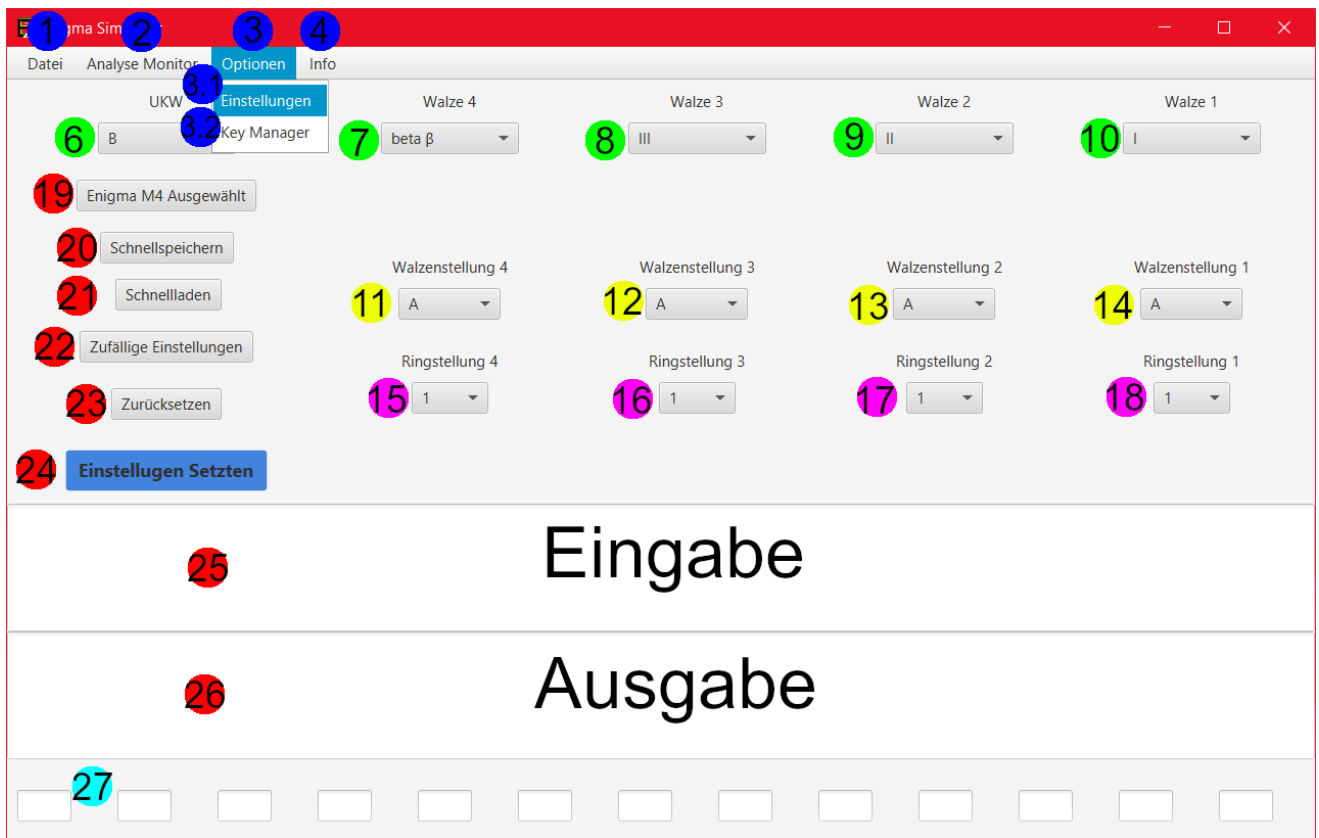
Diese Anwendung ist mit den echten Enigmas M3 und M4 vollständig kompatibel.

Diese Anleitung erklärt nicht die einzelnen Komponenten der Enigma Verschlüsselungsmaschine und ihre Funktion. Diese Informationen sind Drittquellen zu entnehmen. (siehe Punkt 10. Weitere Informationen)

2. Erklärung der Grafischen Benutzeroberfläche



Grafische Benutzeroberfläche nach Start der Anwendung



1. Hier könne die derzeitigen Einstellungen in eine Datei Gespeichert werden oder daraus Geladen werden.
2. Öffnet den Großen oder Kleinen Analyse Monitor.
3. Öffnet das Optionenmenü.
 - 3.1. Öffnet die Einstellungen.
 - 3.2. Öffnet den Key Manager um die derzeitigen Einstellungen in einen Schlüssel Umzuwandeln.
4. Öffnet ein Info Fenster das Informationen zur Anwendung enthält.
6. Auswahl der Umkehrwalze für die Enigma M3 / M4.
7. Auswahl der vierten „Griechenwalze“/ „dünnen Walze“ der Enigma M4 (Nur M4).
8. Auswahl der Dritten Walze für die Enigma M3 / M4.
9. Auswahl der Zweiten Walze für die Enigma M3 / M4.
10. Auswahl der Ersten Walze für die Enigma M3 / M4.
11. Auswahl der Walzenstellung für die vierte Walze für Enigma M4 (Nur M4).
12. Auswahl der Walzenstellung für die dritte Walze für Enigma M3 / M4.
13. Auswahl der Walzenstellung für die zweite Walze für Enigma M3 / M4.
14. Auswahl der Walzenstellung für die erste Walze für Enigma M3 / M4.
15. Auswahl der Ringstellung für die vierte Walze für Enigma M4 (Nur M4).
16. Auswahl der Ringstellung für die dritte Walze für Enigma M3 / M4.
17. Auswahl der Ringstellung für die zweite Walze für Enigma M3 / M4.
18. Auswahl der Ringstellung für die erste Walze für Enigma M3 / M4.
19. Umschalter zwischen Enigma M4 und M3. (Standard M4).
20. Speichert die derzeitigen Einstellungen der Enigma zwischen. (Nur solange Anwendung aktiv)
21. Lädt die zwischengespeicherten Einstellungen wieder in die Oberfläche.
22. Erzeugt Zufällige Einstellungen für die Enigma.
23. Setzt alle Einstellung wieder auf ihren Ursprung (Start) zurück und löscht das Ein- und Ausgabe Feld.
24. Setzt die Einstellung für die Verschlüsselung im Live Modus fest.
25. Eingabe Feld für den zu Verschlüsselnden Text.
26. Ausgabe des Verschlüsselten Textes.
27. Steckbrett Eingabe zwei Buchstaben je Feld die Getauscht werde sollen siehe Steckbrett 3.5.

3. Erklärung der Bedienelemente

3.1. Walzen Auswahl 7. - 10.

Hier können die Walzen bzw. Rotoren die für die Verschlüsselung benutzt werden sollen ausgewählt werden. Dabei lässt sich bei den Rotoren 1 bis 3 zwischen den Walzen I bis VIII (1 – 8) wählen. Bei der Enigma M4 kann auch die vierte Walze die sogenannte Griechenwalzen oder dünne Walze ebenfalls eingestellt werden. Dabei kann zwischen den Walzen Gamma und Beta gewählt werden.

3.2. Umkehrwalze 6.

Hier wird die Umkehrwalze festgelegt dabei kann zwischen B und C gewählt werden.

3.3. Walzenstellung 11. – 14.

Hier wird die Walzenstellung festgelegt. In welcher Position sich die Walze für die Verschlüsselung befindet.

3.4. Ringstellung 15. – 18.

Hier wird die Ringstellung Eingestellt. Dies legt fest um wie viel die interne Verdrahtung des Rotors zum Äußeren Ring verschoben wird.

3.5. Steckbrett 27.

Hier können Buchstaben Kombinationen miteinander „Gesteckt“ / Eingegen werden. Dabei kann in ein Feld eine Buchstaben Kombination aus zwei Buchstaben eingeben werden die miteinander verbunden bzw. getauscht werden soll (Gesteckt). Dabei ist darauf zu achten das sich kein Buchstabe in einem anderen Feld Wiederholt.

3.6. Umschalter Enigma M4 / M3 19.

Mit diesem Button kann zwischen der M4 und M3 Version der Enigma umgeschaltet werden. Standardmäßig ist die Enigma M4 mit ihren 4 Rotoren ausgewählt. Die M3 Version besitzt hingegen nur 3 Rotoren und die vierte Walze fällt weg und wird auch ausgegraut. Der Schalter zeigt auch den Status in Schrift und visuell an. Ist dieser gedrückt wird dieser grau hinterlegt was anzeigt das, die M3 ausgewählt ist.

3.7. Schnellspeichern / Schnellladen 20.

Schnellspeichern speichert die derzeitigen Einstellungen der Enigma zwischen um diese mit dem Schnellladenbutton wieder laden zu können. Aber nur solange der Simulator aktiv ist nach dem beenden gehen die gespeicherten Einstellungen verloren. Auch werden nur die Einstellungen nicht jedoch Eingabe und Ausgabe gespeichert.

3.8. Zurücksetzen 23.

Setzt die Einstellung wieder in die Grundeinstellungen zurück und löscht das Ein- und Ausgabe Feld.

3.9. Einstellungen setzen 24.

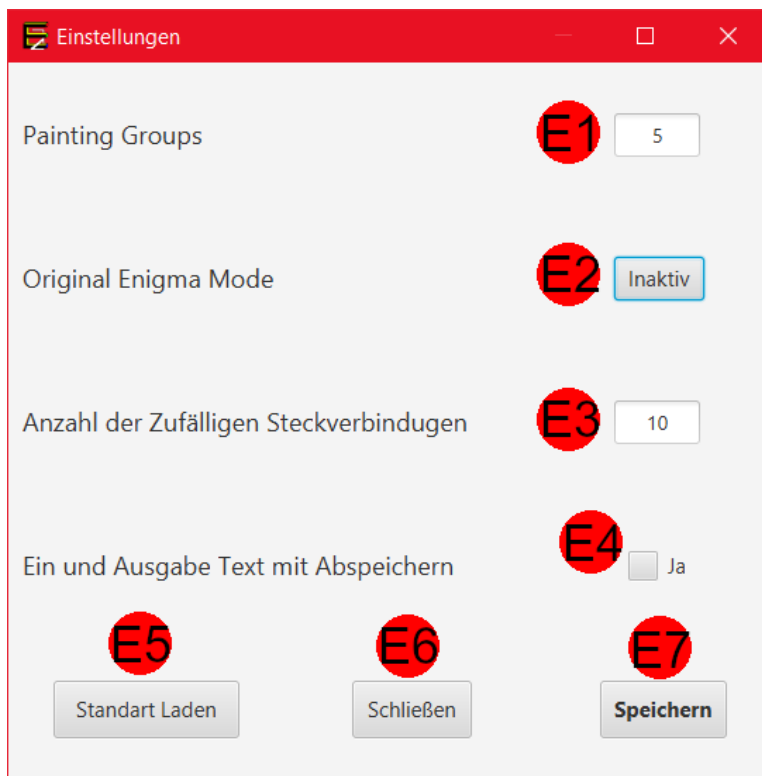
Im Live Modus muss nach dem Einstellen der Enigma aber vor dem Verschlüsseln dieser Button betätigt werden, um die Einstellungen für die Verschlüsselung wirksam werden zu lassen. Sollten im Nachhinein Änderungen an den Einstellungen der Enigma vorgenommen werden muss dieser Button erneut betätigt werden.

Im Original Modus entfällt dieser Schritt. Der Button ist auch nicht betätig bar.

3.10. Zufällige Einstellungen Erzeugen 22.

Erzeugt zufällige Einstellungen, für die Enigma die für die Verschlüsselung genutzt werden können. Die Anzahl der zufälligen Steckverbindungen ist ein den Einstellungen Konfigurierbar (E3). Die Betätigung des „Einstellungen setzen“ (24.) Buttons entfällt nach Betätigung des Buttons ist die Enigma einsatzbereit.

4. Erklärung der Einstellungen



E1. Einstellung zu wie vielen Gruppen an Buchstaben der Verschlüsselte Text ausgegeben werden soll. Standard ist 5.

E2. Aktiviert den Enigma Original Mode oder Wechselt wieder zurück in den Live Modus. Standard Inaktiv (Live Modus). Das wechseln des Modus setzt die Oberfläche und Einstellungen der Enigma zurück!

E3. Anzahl der Zufälligen Steckverbindungen die bei der Erzeugung von zufälligen Einstellungen erzeugt werden sollen. Standard ist 10 da dies die Höchste Sicherheit bietet. Maximalwert 13

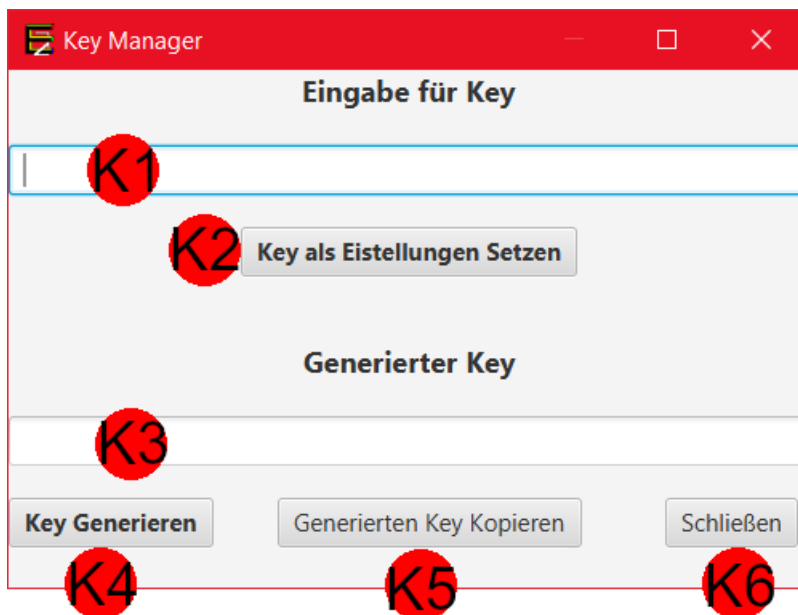
E4. Ist dieser Haken gesetzt werden beim Speichern der Einstellungen der Enigma in eine Datei über das Menü (1.). Die Ein- und Ausgabe Texte mit abgespeichert. Standard nicht gesetzt.

E5. Lädt die Standard Werte der Einstellungen und Speichert diese.

E6. Schließt dieses Einstellung Fenster.

E7. Speichert die vorgenommenen Einstellungen.

5. Erklärung des Key Manager Systems (Einstellungen zu Schlüssel)



K1. Eingabe Feld für einen Einstellungs Key / Schlüssel der als Einstellungen für die Enigma verwendet werden soll.

K2. Überführt den Eingebenen Key aus dem K1. Feld in Einstellungen für die Enigma. Bei Erfolg schließt sich dieses Fenster.

K3. Feld für den aus Einstellung der Enigma Generierten Key.

K4. Generiert aus Einstellungen der Enigma die im Haupt Fenster gesetzt wurden einen Schlüssel in das Feld K3.

K5. Kopiert den Generierten Schlüssel in die Zwischenablage des Betriebssystems.

K6. Schließt dieses Fenster.

6. Laden und Speichen von Einstellungen

Mittels des Menüpunktes „Laden / Speichen“ (1.) können die derzeitigen Einstellungen der Enigma sowie auch der Fortschritt der Verschlüsselung in eine Datei gespeichert werden.

Zum Speichern wird unter dem Menüpunkt 1. „Speichern“ ausgewählt und ein Speicherort festgelegt. Außerdem kann die Ein- und Ausgabe mit abgespeichert werden. Dies ist jedoch vor dem Speichern in den Einstellungen unter Punkt (E4) einzustellen. Außerdem wird der Verwendete Modus mit abgespeichert und beim laden auch wieder in diesen gewechselt.

7. Erklärung des Original Enigma Mode

Der Original Enigma Mode dient dazu den Enigma Simulator wie eine echte Enigma in der Realität zu benutzen. So entfällt die Notwendigkeit des Einstellung setzten Buttons (24.) und Änderungen an den Einstellungen werden sofort wirksam. D.h. jedoch auch das während der laufenden Verschlüsselung die Einstellung nicht geändert werden sollten. Auch wird im Eingabefeld die Eingabe nicht länger mit angezeigt nach jeder Eingabe wird diese gelöscht. Nur im Ausgabe Feld wird das Ergebnis der Verschlüsselung angezeigt.

Im Original Modus stehen außerdem die Analyse Monitoren nicht zur Verfügung.

Das Laden und Speichern von Einstellungen ist jedoch mit Schnellspeichern, Speichern der Einstellungen in eine Datei und dem Key System weiterhin möglich.

Durch den Wechsel des Modus in den Einstellungen ist zu beachten das alle Einstellungen der Enigma in der Oberfläche zurückgesetzt werden.

8. Erklärung Analysemonitor

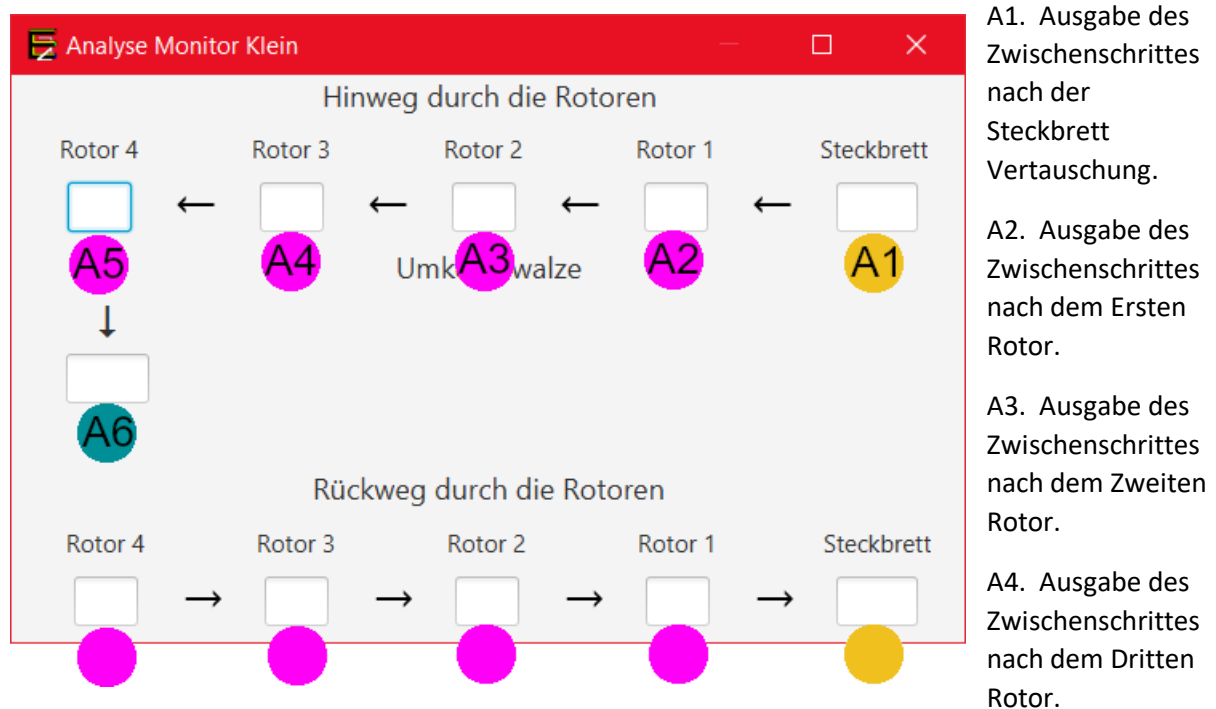
Der Analysemonitor zeigt die Arbeitsweise der Enigma und wie die Verschlüsselung im genauen funktioniert.

Dabei unterteilt sich der Analysemonitor in zwei verschiedene Varianten. Einmal den Kleinen Analyse Monitor um einen groben Überblick über die Verschlüsselungsverfahrensweise der Enigma zu erhalten. Dieser zeigt wie eine Walze einen Buchstaben in einen anderen tauscht.

Der Große Analysemonitor zeigt hingegen die exakt genaue Arbeitsweise des Implementierten Verschlüsselung Algorithmus. Beziehungsweise die mechanische Abbildung der Enigma in Programmcode. Außerdem wird hierbei die abstrakte und genaue Arbeitsweise der Enigma deutlich. So lassen sich im Großen Analysemonitor selbst Dinge ablesen die nur die Theoretische und mathematische Arbeitsweise der Enigma widerspiegeln. So wird hierbei auch der Versatz der Ringe an den Rotoren deutlich, der selbst bei einer echten Enigma nicht zum tragen kommen würde, weil dieser schon durch die mechanische Bauweise berücksichtigt ist. Der Vorteil des Algorithmus mit seiner hohen Informationsdichte wird hier besonders deutlich und seine Arbeitsweise kann damit sehr genau verfolgt werden.

Im Enigma Original Modus steht der Analyse Analysemonitor nicht zur Verfügung!

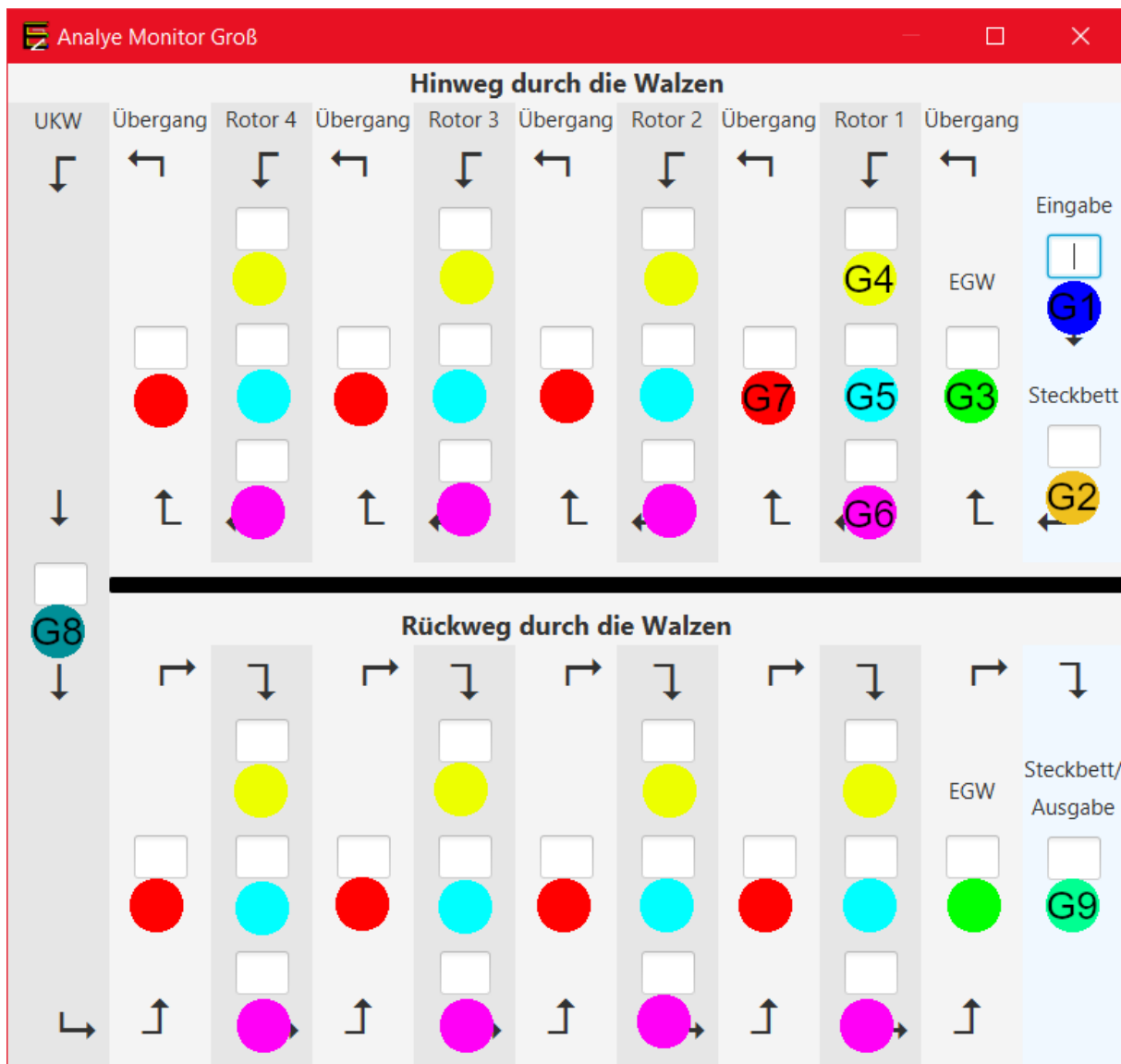
Falls der Enigma M3 Modus ausgewählt wurde werden die Felder für den vierten Rotor nicht genutzt und können übersprungen werden. Die Felder die somit Leer bleiben sind somit als nicht existent anzusehen.



A5. Ausgabe des Zwischenschrittes nach dem Vierten Rotor nur im Enigma M4 Modus eine Ausgabe enthalten.

A6. Ausgabe des Zwischenschrittes nach der der Umkehrwalze.

Die Elemente die gleichfarbig gekennzeichnet sind analog zu den Beschrifteten anzusehen nur als Rückweg durch Walzen.



G1. Eingegebener Buchstabe

G2. Ausgabe des Zwischenschrittes nach der Steckbrett Vertauschung.

G3. Abgleich der Stellung der Eingabe Walze (EGW) zum ersten Rotor zur richtigen Übertragung des Buchstabens.

G4. Abgleich der Ring Verschiebung des Rotors um den Buchstaben richtig mit der Internen Verdichtung zu vertauschen.

G5. Eigentliche Verschlüsselung hier wird der Buchstabe durch die Rotor Verdrahtung getauscht.

G6. Abgleich der Ring Verschiebung des Rotors um den Buchstaben wieder richtig, um die Verschiebung des Ringes zu tauschen. (Gleich wie G4. nur Umgekehrt)

G7. Abgleich der Stellung von Rotor 1 und Rotor 2 um den Buchstaben korrekt an den Rotor 2 zu Übergeben.

G8. Ausgabe des Zwischenschrittes nach der der Umkehrwalze.

G9. Ausgabe der Verschlüsselung nach dem Steckbrett bzw. das Ergebnis der Verschlüsselung.

Die Felder die gleichfarbig gekennzeichnet sind analog zu den Beschrifteten anzusehen. Jedoch handelt es sich hierbei um andere Rotoren siehe Beschriftung Oberfläche.

9. Beispiel für eine Verschlüsselung / Vorgehen bei einer Ver- oder Entschlüsselung

Hier das Beispiel für einen Verschlüsselungsablauf im Live Modus.

1. Entscheiden ob M4 oder M3 benutzt werden soll.
2. Optional Eingabe Feld, wenn dies bereits etwas enthält leeren.
3. Optional vorherige Einstellungen mit „Zurücksetzen“ (23.) löschen. (Empfohen)
4. Optional Einstellungen Laden mit Schnellladen, aus Datei oder aus Key. (Alle Punkte bis 10. Entfallen)
5. Einstellungen an der Enigma vornehmen.
 - a. Walzen auswählen (7. – 10.).
 - b. Umkehrwalze (UKW) festlegen (6.).
 - c. Walzenstellung festlegen (11-14.).
 - d. Ringstellung einstellen (15.-18.).
 - e. Steckbrett Eingeben (27.).
 - i. Die Buchstaben Kombination die gesteckt werden soll in das Feld eingeben z.B.: Feld 1 [IF] (dabei wird I mit dem Buchstaben F getauscht).
 - ii. Keine doppel oder mehrfach eingaben tätigen z.B: nicht Feld 1 [AK] und Feld 2 [KA] oder Feld 1 [SD] Feld 2 [DA] ebenfalls nicht Feld 1 [LL]. dies eingaben repräsentieren doppel Eingaben und sind nicht zulässig.
 - iii. In welche Richtung gesteckt / Einggegeben wird ist dabei egal z.B.: repräsentieren Feld 1 [TR] oder [RT] dieselbe Steckverbindung bzw. Eingabe. Auch ist die Reihenfolge wie gesteckt wird egal.
6. Auf den Button „Einstellungen Setzen“ (24.) klicken um die Einstellungen zu setzten und wirksam werden zu lassen.
7. Optional Einstellungen mit Schnellspeichern zwischen Speichern. (20.)
8. Optional Einstellungen In eine Datei Exportieren. (1.)
9. Optional einen Key aus den Einstellungen mit dem Key Manager erstellen. (4.)
10. Text zum Ver- / Entschlüsseln in das Eingabefeld eingeben.
11. Ver- / Entschlüsselten Text lesen / kopieren.

Im Enigma Original Mode Entfällt nur der Schritt 6 und es kann nach dem Einstellen sofort verschlüsselt werden.

Falls die Einstellungen mit dem Zufällige Einstellungen Button (22.) Erzeugt werden entfällt Schritt 5 mit all seinen Unterpunkten und Schritt 6. Außer es soll Manuell an den Zufälligen Einstellungen noch etwas geändert werden.

Beispiel Text zum Entschlüsseln

Einstellungen:

Enigma M4

Walze 1: III

Walze 2: I

Walze 3: VII

Walze 4: gamma

UKW: C

Walzenstellung der Walze 1: K

Walzenstellung der Walze 2: W

Walzenstellung der Walze 3: A

Walzenstellung der Walze 4: P

Ringstellung der Walze 1: 2

Ringstellung der Walze 2: 17

Ringstellung der Walze 3: 10

Ringstellung der Walze 4: 5

Steckbrett:

BA

OL

ZP

TG

XR

EY

WS

Key für diese Einstellungen: 9vd895QmcmqHYvHCubmC6smqQMh9S2La8LDxGoZ6iMr7Jvx

Zu Entschlüsselnder Text:

BPUVL MIELU QGTUI MQTUF DGUYA QJHIB GUIYU DYZKE SGZWK ZJRGH KFYND YDUHE
USGDQ KLHGC TJUGR GNZOK GTABB JPYNT CPEQS JACIN W

Zu beachten ist, dass wie bei einer echten Verschlüsselung mit der Enigma die Leerzeichen durch X repräsentiert werden.

10. Informationen Zur Installation

Das Programm benötigt keine Installation die JaS-Enigma_Simulator.jar kann sofort gestartet werden.

Zur Ausführung des Programms wird jedoch das Java SE Runtime Environment mindestens Version 8 benötigt.

Bei der Installation des Java SE ist jedoch darauf zu achten das die JavaFX Komponenten mit installiert werden. Bei neueren Java Versionen werden diese teils einzeln ausgeliefert und sind entsprechend nach zu installieren.

11. Weitere Informationen

Informationen zu den einzelnen Komponenten und ihrer Funktion der Enigma Verschlüsselungsmaschine sind zu finden unter:

<http://gocs.info/archiv/DiplomArbeit.pdf>

<http://www.softdoc.de/mr/de/downloads/files/EnigmaTechnischeDetails.pdf>

[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)](https://de.wikipedia.org/wiki/Enigma_(Maschine))

Achtung aufgrund von nicht Gelösten Bugs im JavaFX unter Linux kann es zu Anzeige Fehlern oder zu Abstürzen des Programms bei der Ausführung unter Linux kommen.

Eine Funktion Garantie unter Linux kann somit leider nicht gewährleistet werden.

Zum Überprüfen der Korrektheit / Testen der Enigma siehe. <http://people.physik.hu-berlin.de/~palloks/js/enigma/>

12. Lizenz (CC-BY-4.0)

Copyright (C) 2020-2021 Jasley Jangk | Github @JaSicX All rights reserved.



Diese Bedienungsanleitung ist lizenziert unter der Creative Commons Attribution 4.0 International Public License.

Links zur Lizenz:

Deutsch: <https://creativecommons.org/licenses/by/4.0/legalcode.de>

Englisch: <https://creativecommons.org/licenses/by/4.0/legalcode>