

Enigma

Briefing

Die Idee dieses Programmes soll sein, eine Enigma Rotorschlüsselmachine zu erstellen, welche Code verschlüsseln kann aber auch entschlüsseln kann.

Da die Aufgabenstellung sehr umfangreich ist wird hier nur auf die wesentlichen Punkte eingegangen und eine sehr abgespeckte Version einer Enigma Maschine zu programmieren sein.

Die Walzenstellungen finden Sie in einem weiterführenden Textfile „Walzenstellung.txt“.

Walzen

Eine Enigma Maschine besteht bekanntlich aus drei Rotoren (plus Umkehrrotor) im Folgenden als Walzen bezeichnet von links nach rechts nummeriert mit römischen Buchstaben I, II, III. Nach den drei Walzen gibt es eine Umkehrwalze (UKW), welche den Input umdreht und wieder durch die drei bestehenden Walzen schickt. Die Permutation der einzelnen Walzen sei als gegeben anzunehmen.

Jede Walze hat eine Startposition. Von dieser ausgehend wird mit jedem Tastenanschlag, die Walzenposition der rechtesten Walze (III) um eins weitergeschoben. Wurde dies 26-mal gemacht, wird die mittlere Walze (II) um eins weitergedreht. Wurde nun 26*26 weitergedreht, wird die linke Walze (I) um eins weitergedreht.

Unter Weiterschieben wird verstanden, dass der nächste Eingang genommen wird. z.B. ABC ergibt permutiert HXK. So würde bei der ersten Eingabe von A ein Ausgang von H einstellen. Danach wird die Walze gedreht und der die Walzenposition erreicht die Stellung BCA mit der Permutation XKH. Gibt man nun noch ein A ein wird dieses in die Walze als vermeintliches B eingepflegt und ergibt als Ausgang ein X usw.

Der Ausgang einer Walze ist der Eingang der nächsten Walze mit Ausnahme der UKW welche 13 Fixverbindungen in der Walze selbst beinhaltet. z.B. A->Z usw.

Danach geht der Vorgang wieder von vorne los nur beginnend mit der Walze I.

Es werden immer drei Walzen aus einem Set von fünf Walzen gewählt. Bei den Umkehrwalzen sind UKW A, UKW B sowie UKW C verfügbar. Die drei Walzen können zudem in jeweils 6 verschiedenen Positionen verbaut sein. Außerdem ist der Startwert variabel, ebenso wie die Weiterschaltung für die weiteren Walzen, sowie auch ob es auch noch eine zweite Weiterschaltung gibt z.B. beim Buchstaben G und beim Buchstaben W.

Steckerbrett

Nach den Walzen kommt der so permutierte Buchstabe zum Steckerbrett, welches Wahlweise einen Buchstaben auf einen anderen legt oder eben diesen weiterreicht. Dieser umgelegte Buchstabe wird immer umgelegt, so wird also bei einer Steckerverbindung AC der Buchstabe A immer durch den Buchstaben C getauscht und der Buchstabe C durch den Buchstaben A.

Es sind bis zu 10 Verbindungen möglich.

Anschließend wird dieser vermeintlich getauschte Buchstabe erneut durch die Walzen gejagt, um dann das entsprechende Lämpchen zu betätigen.

Umkehrung

Da Die Eingabe bei selber Startposition immer denselben Ausgang liefert und umgekehrt, ist eine Umkehrung nicht weiter nötig und automatisch mit eingebaut.

Aufgabenstellung

Phase 1

Erstellen Sie nun eine abgespeckte Version einer Enigma Maschine.

Fokussieren Sie sich zuerst auf eine Walze und sorgen Sie dafür, dass Sie eine Methode haben, welche diese Walze bei jeder Betätigung um eine Position verschiebt.

Phase 2

Wenn Sie das bewerkstelligt haben, erstellen Sie sich eine Umkehrwalze, welche den Eingang umlenkt.

Kombinieren Sie nun Ihre so erstellte Walze I mit Ihrer UKW A.

Versuchen Sie dann mit gleicher Ausgangsstellung der Walze I einmal den Code zu verschlüsseln und denselben Code zu entschlüsseln. Im besten Fall funktioniert dies einwandfrei.

Phase 3

Erstellen Sie nun auch noch eine Walze II sowie III und kombinieren Sie diese mit der Walze I sowie UKW A. Auch hier sollte bei gleicher Ausgangsstellung sowohl eine Ver/Entschlüsselung möglich sein.

Phase 4

Erstellen Sie nun unabhängig der Phasen 1-3 die Phase 4 welche die Steckerverbindungen realisieren soll. D.h. eine Eingabe von AC tauscht die Buchstaben A und C am Steckerbrett.

Phase 5

Verbinden Sie nun Phase 4 mit den Phasen 1-3 und schicken Sie diesen so generierten Buchstaben erneut durch alle drei Walzen, die UKW und retour durch die drei Walzen.

Erweiterung

Lassen Sie nun den Benutzer drei Walzen aus fünf Walzen wählen.

Ebenso soll der Benutzer weitere Walzen erstellen können. Auch UKWs.

Härtepunkt

Als veränderliche Werte sind nun anzunehmen:

- Walzen inkl. UKW sowie deren Steckposition
- Startposition der Walzen
- Weberschaltungspunkt der Walzen
- Steckerbrettverbindungen

Lassen Sie diese Einstellungen in Ihrem Programm zu!

Walzenschaubild

