



Softwarepraktikum: Enigma

Sommersemester 2003

Handout 5

14. April 2003

Handout 5: Details zur Enigma

Ausgabetermin: 14. April 2003

Der Zettel enthält ein paar weitere Erläuterungen zur Enigma und speziell dem Aufbau der Walzen. Die Bilder sind von der *Code and Ciphers* Homepage genommen.

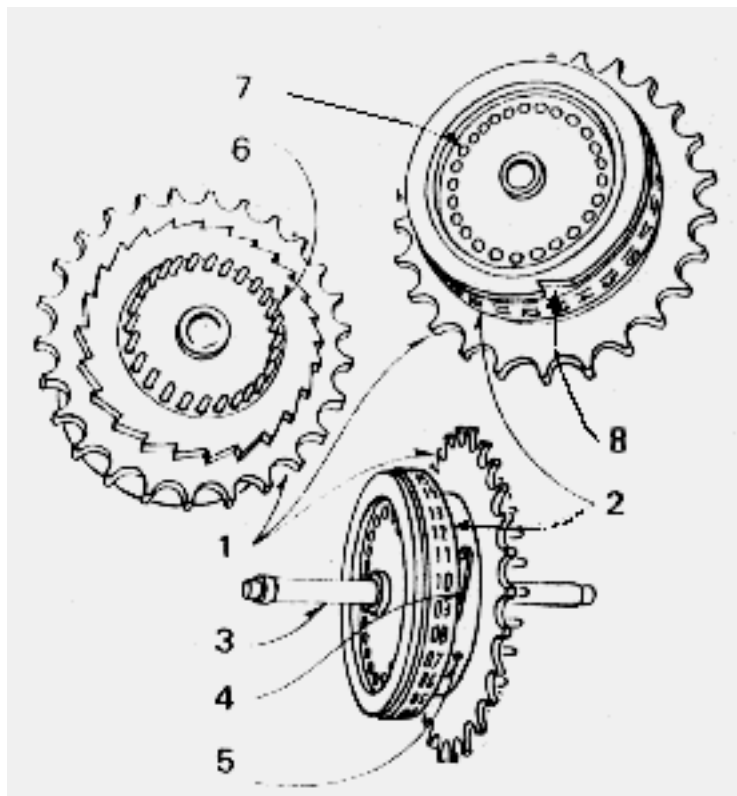


Abbildung 1: Walzenaufbau

Die Komponenten auf der Zeichnung sind:

1. Fingerkerben; dort stellt der Benutzer an der geschlossenen Enigma die Stellung der Walzen ein.
2. der Alphabetring
3. die Achse
4. Verschlußvorrichtung, um den Alphabetring mit dem Kern zu verbinden
5. der Walzenkern, der die "Permutation" von den Endkontakten auf beiden Seiten der Walze enthält (Punkte 6 und 7)
6. Stiftkontakte
7. Kontakt
8. *Übertragskerbe*, am Alphabetring angebracht

Wichtig ist die Trennung von Ring und dem Kern, d.h., daß der Ring sich *relativ* zum Kern, der die eigentliche Verdrahtung d.h., Permutation enthält, eingestellt werden kann. Ferner ist wichtig, daß der *Übertragsmechanismus* nicht mit dem Walzenkern verbunden ist sondern mit dem *Ring*. Genauer gesagt wird der Übertrag durch die Übertragskerbe bestimmt (Punkt 8). Diese Kerbe ist für jeden der vorhandenen Walzen an anderer Stelle.

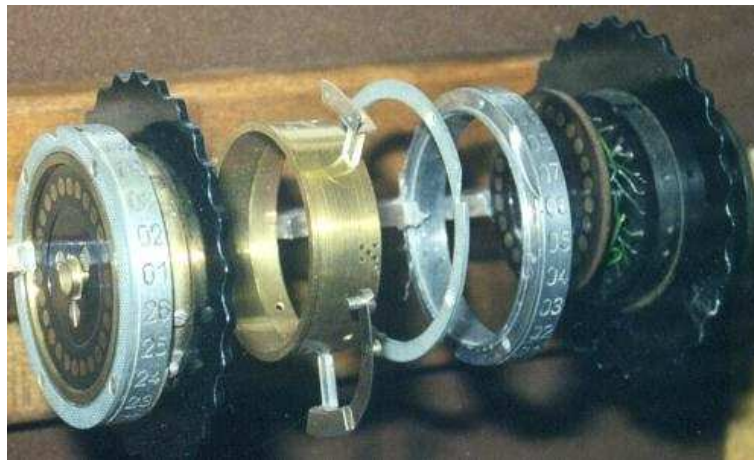


Abbildung 2: Zerlegte Walze

Übertragunsanomalie

Beachten Sie bitte bei Ihrer Realisierung auch auf die sogenannte *Übertragunsanomalie*. Die Rotoren der Enigma funktionieren nicht 100% gleichförmig was den Übertrag betrifft. Der letztliche Grund liegt dabei in der mechanischen Realisierung des Übertrags zwischen den Walzen.

Außer daß die physikalischen Gegebenheiten zum Verständnis beitragen, sind wir letzten Endes natürlich nur an der “Logik” der Anomalie interessiert.

Die Rotoren sind so angeordnet, daß die Walze rechts am schnellsten rotiert, und zwar bei jedem Tastendruck um eine Position. Ganz präzise rotiert die Walze *bevor* die Verschlüsselung durchgeführt wird.

Der Übertrag wird mittels eines T-förmigen Stössels (*“pushrod”*) durchgeführt der in die Übertragskerben passt. Die Anomalie betrifft (bei der 3-Walzen Version der Enigma) die mittlere und die linke Walze, also die zwei langsamen.¹ Sie führt dazu, grob gesagt, daß es passieren kann, daß der mittlere Rotor *2 mal hintereinander* rotiert. Dann nämlich wenn er —das erste mal— regulär von dem schnellen, rechten Rotor “mitgenommen” wird und danach im kommenden Schritt den linken im Zuge eines weiteren Übertrags selbst “mitnimmt”.

¹Ganz streng genommen ist mechanisch auch die rechte Walze betroffen, aber da sie sich ohnehin jedesmal bewegt, bleibt die Anomalie unbemerkt.