

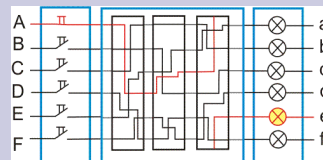
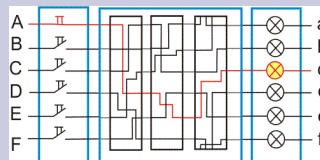
# Chiffriermaschine ENIGMA

## Fachpräsentation Informatik

### Das Rätsel der ENIGMA

Die ENIGMA wurde von ARTHUR SCHERBIUS im Jahr 1923 entwickelt. Sie besteht aus einer oder mehreren Walzen, einer Tastatur und verschiedenen Lampen, die jeweils einen Buchstaben darstellen. Durch die Tastatur wird ein elektrischer Impuls gesandt und je nach Walzenstellung zu einer anderen Lampe geleitet. Zur Veranschaulichung zeigen die beiden Abbildungen das an 3 Walzen mit 6 Buchstaben.

In der linken Abbildung wurde auf die Taste **A** gedrückt und durch die Walzenstellung leuchtet die Lampe vor **C**. Bisher noch nichts besonderes, nur eine monoalphabetische Verschlüsselung, aber jetzt kommt der Trick. Die Walze wird nach jedem Buchstaben automatisch um eine Position weitergedreht. Wenn man also das nächste Mal auf **A** drückt, so bekommt man ein **e** (rechte Abb).



Den wichtigsten Teil der Verschlüsselungseinheit bildeten zunächst 3 Walzen, später sogar 4 Walzen, die aus insgesamt 5 bzw. 8 Walzen ausgewählt und in die Maschine eingesetzt wurden. In jede Walze führten 26 Drähte, zusätzlich ließ sich jede Walze in 26 Stufen (eine für jeden Buchstaben des Alphabets) drehen. Insgesamt entsteht durch die elektrischen Schaltungen in den Walzen eine polyalphabetische Verschlüsselung mit sehr vielen Möglichkeiten. Die Anzahl der Permutationen erhöhte man durch das sog. Steckbrett weiter. Der gesamte Schlüsselraum einer ENIGMA mit drei aus einem Vorrat von fünf ausgewählten Walzen und einer von zwei Umkehrwalzen sowie bei Verwendung von zehn Steckern lässt sich mit 120 Walzenlagen, 676 Ringstellungen, 17576 Grundstellungen und 150.738.274.937.250 Steckmöglichkeiten berechnen. Er beträgt 214.917.374.654.501.238.720.000.

### Bedienung der ENIGMA

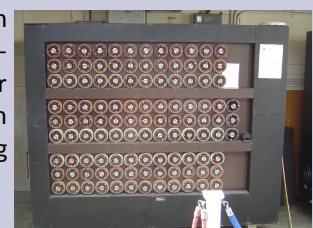
Zunächst mussten die richtigen Walzen, und die korrekte Umkehrwalze ausgewählt werden. Die Walzen wurde in einer

Tag	UKW	Walzenlage	Ringstellung	Steckerverbindungen
31	B	I IV III	16 26 08	AD CN ET FL GI JV KZ PU QY WX
30	B	II V I	18 24 11	BN DZ EP FX GT HW IY OU QV RS
29	B	III I IV	01 17 22	AH BL CX DI ER FK GU NP OQ TY

festgelegten Reihenfolge auf eine Achse montiert und in die Maschine eingesetzt. Nun musste die Ringstellung eingestellt werden, also die Verschiebung der Buchstabenreihenfolge auf einer Walze. Anschließend wurde die Verbindungen des Steckbretts gesteckt. Nun musste der Spruchschlüssel ermittelt und eingestellt werden. Erst jetzt war der Funker bereit, die Nachricht zu dekodieren.

### Entschlüsselung der ENIGMA

Trotz der immensen Anzahl an Kombinationen gelang es erstmalig dem Polen MARIAN REJEWSKI die ENIGMA-Verschlüsselung zu brechen. Dies gelang ihm u. A. dadurch, dass er Zugang zu einer Bedienungsanleitung der deutschen Maschine hatte. Seine Arbeiten wurden während des Zweiten Weltkrieges von den Briten in Bletchley Park bei London unter Führung von Alan Turing — dem Vater des Computers fortgeführt.



### Quellen für Text und Bilder:

- Seite „Enigma (Maschine)“. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 4. März 2013, 06:23 UTC. URL: [http://de.wikipedia.org/w/index.php?title=Enigma\\_\(Maschine\)&oldid=114944125](http://de.wikipedia.org/w/index.php?title=Enigma_(Maschine)&oldid=114944125) (Abgerufen: 5. März 2013, 09:12 UTC)
- Turing-Bombe. T. Hempel