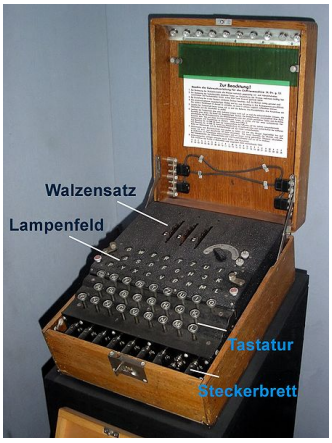
Rotoren

Substitution (polyalphabetisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. **Was** sie sind, ist immer wieder verschieden.
Solche Verschlüsselungen heißen **polyalphabetische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Poly* heißt *viel*.)



Die berühmteste Rotor-Maschine zur Verschlüsselung ist die **ENIGMA**, die vom deutschen Militär im zweiten Weltkrieg eingesetzt wurde. Das Wort »Enigma« kommt aus dem Griechischen und bedeutet »Rätsel«. Das Prinzip beruht auf einer drehbaren Scheibe, die jeden Buchstaben durch einen anderen ersetzt, dann gedreht wird und nun jeden Buchstaben durch einen anderen als zuvor ersetzt. Die Enigma hatte mehrere Scheiben. Sie wurde erst nach einigen Jahren durch intensive mathematische Forschung geknackt.

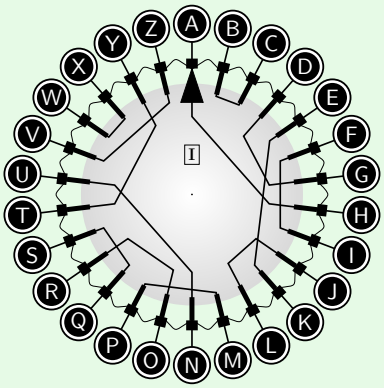
So wird mit Rotoren verschlüsselt:

- Sender und Empfänger einigen sich auf einen Schlüsselbuchstaben.
- Der Rotor wird so eingestellt, dass der Pfeil auf den Schlüsselbuchstaben zeigt.
- Jeder Buchstabe der Nachricht wird durch den Buchstaben ersetzt, der sich am anderen Ende der auf dem Rotor eingezeichneten Verbindung befindet.
- Immer, wenn du einen Buchstaben verschlüsselt hast, wird der Rotor im Uhrzeigersinn eine Position weiter gedreht.

Zum Entschlüsseln muss erneut der Schlüsselbuchstabe eingestellt werden, dann wird von vorn bis hinten entschlüsselt.

Beispiel

Der Schlüsselbuchstabe ist hier »A«. Möchtest du nun den Buchstaben »S« verschlüsseln, so folgst du der Linie bei »S« und landest bei »Q«. Dann wird der Rotor um eine Position nach rechts gedreht, der Pfeil steht nun auf dem B. Dann verschlüsselst du den nächsten Buchstaben. Die Verbindungen der Buchstaben haben sich nun auch verschoben, so dass z. B. als zweiter Buchstabe ein »C« durch ein »D« verschlüsselt wird.



v3 5. Juli 2013