78 97 99 104 114 115 99 104 116

Verschlüsselung von Informationen

Warum Verschlüsselung ?

- Geheimhaltung der Information
- Wahrung der Anonymität
- Echtheit einer Information
- Sicherheit

In der Wissenschaft nennt man das Gebiet der Verschlüsselung **Kryptologie.**

Das Entschlüsseln einer Information ohne Kenntnis des Verschlüsselungsverfahrens nennt man **Kryptoanalyse**.

Versteckt man (geheime) Informationen in anderen Informationen (z.B. in Grafiken) so spricht man von ***Steganographie****.*

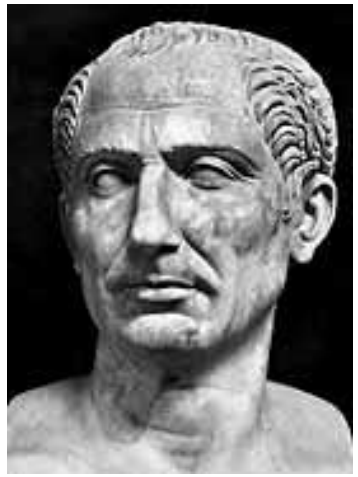
Bei einer Textverschlüsselung werden die Zeichen des Textes durch andere Zeichen ersetzt oder in ihrer Reihenfolge vertauscht.

Zum Ver- und Entschlüsseln einer Nachricht sind die Wahl und Kenntnis eines **Schlüssels** notwenig.

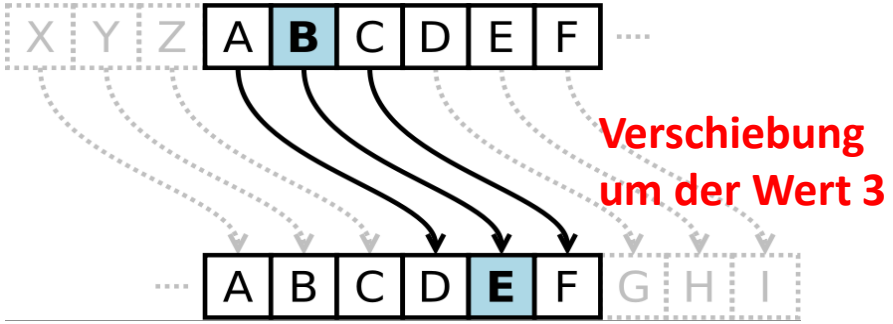
Verschlüsselung im Altertum:

Julius Cäsar
(römischer Feldherr)

ca. 100 J.v.u.Z

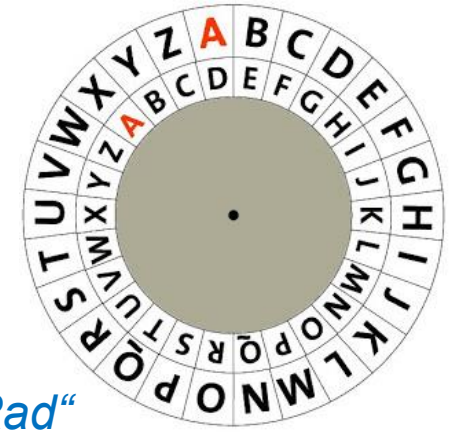


Skytale - der Stock



Ältestes bekanntes militärisches Verschlüsselungsverfahren, welches vor mehr als 2500 Jahren von den Spartanern (Griechen) genutzt wurde.

Die Buchstaben des Klartestes werden im Alphabet um einen bestimmten Wert verschoben



„Cäsar-Rad“

Verschlüsselung in der Gegenwart:

= Rätsel

Rotorverschlüsselungsmaschine, die im 2.Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs im Militär, Polizei und Geheimdienst eiungesetzt wurde

→ *trotzdem gelang es die Informationen zu entziffern*

Heute erfolgen Verschlüsselungen mit Maschinen (Computern).

Es existieren sehr viele verschiedene Verschlüsselungsverfahren.

→ *Informatikunterricht Klasse 12*

► **Jede Verschlüsselung kann heute „geknackt“ werden.**

► **Es gibt keine absolute Sicherheit !**

Mit Hilfe des Cäsar-Codes (und der Tabellenkalkulation) sollen folgende Ver- und Entschlüsselungen vorgenommen werden.

1. Verschlüssele deinen Namen mit dem Cäsar-Schlüssel S=3.

2. Entschlüssele die Information:

Q e y p { y v j

mit dem Cäsar-Schlüssel S=4.

3. Entschlüssele die folgende Information (Finde den Schlüssel):

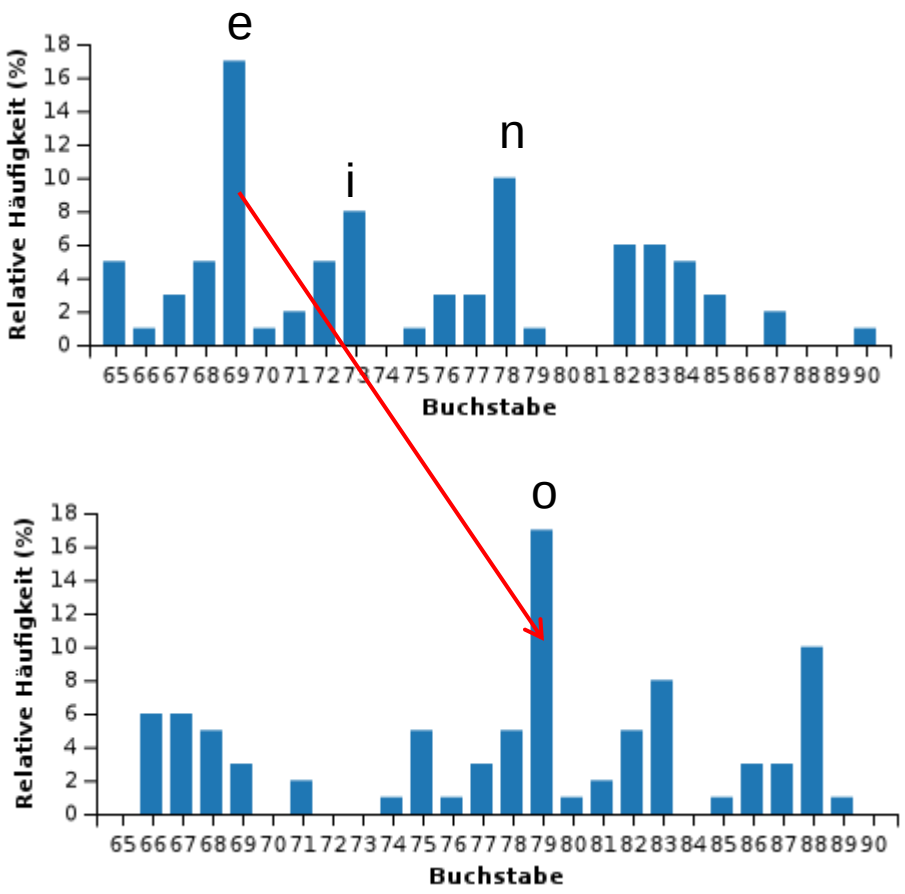
L j m j n r

4. a) Schreibe deinem Banknachbarn eine verschlüsselte Nachricht auf Papier (mit bzw. ohne Angabe des Schlüssels).
Verwende als Trennzeichen zwischen den Worten /.
b) Entschlüssele die erhaltene Nachricht deines Banknachbars.

Entschlüsselung des Cäsar-Codes:

(1) Ausprobieren verschiedener Schlüssel

(2) Buchstabenhäufigkeit der Sprache



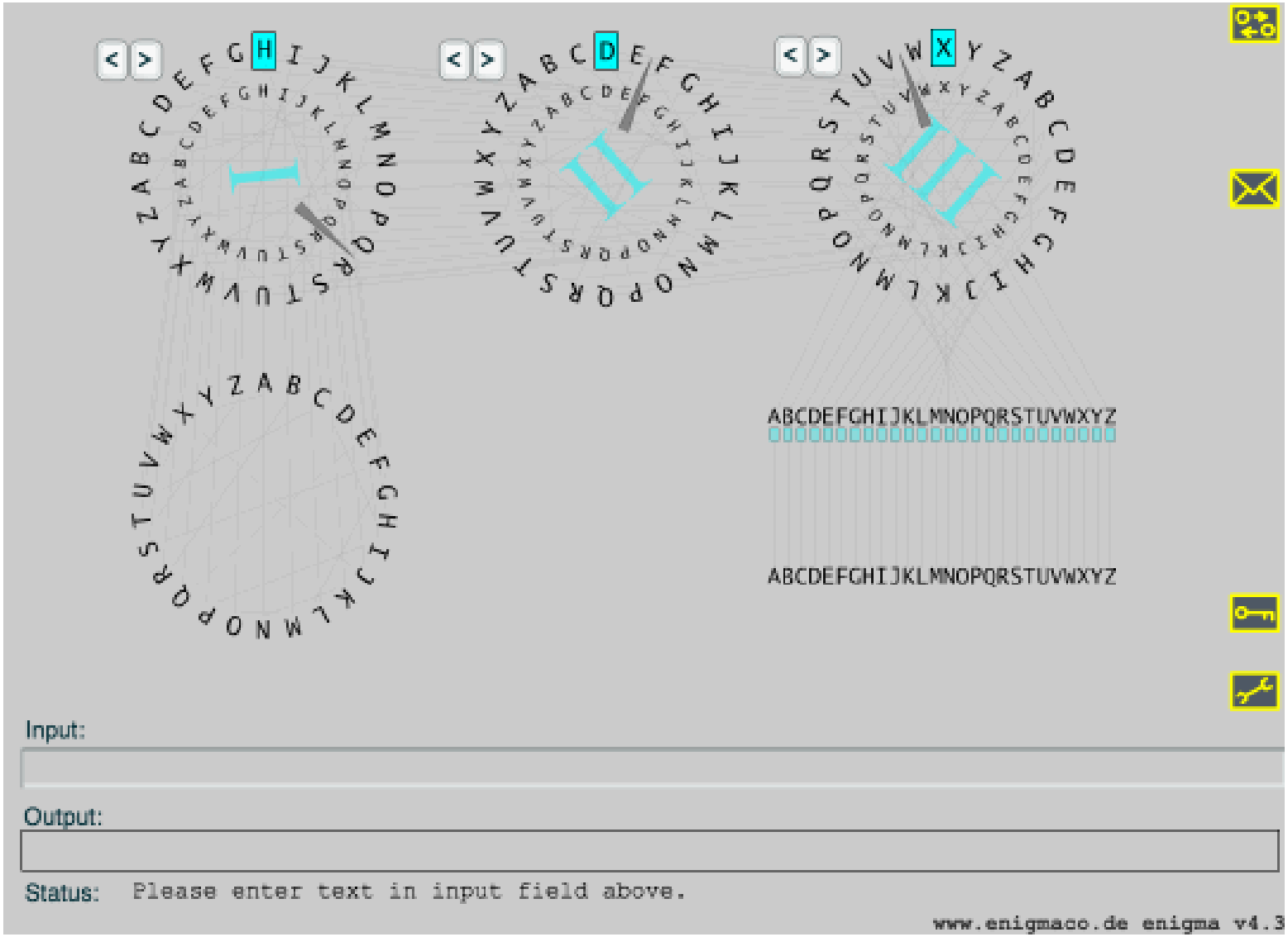
Der häufigste Buchstabe in (längeren) deutschen Texten ist „e“, gefolgt von „n“ und „i“.

Die Zuordnung der Häufigkeit im verschlüsselten Text lässt den Schlüssel erkennen.

e → o

Schlüssel: 10

Der Enigma-Code:



Link