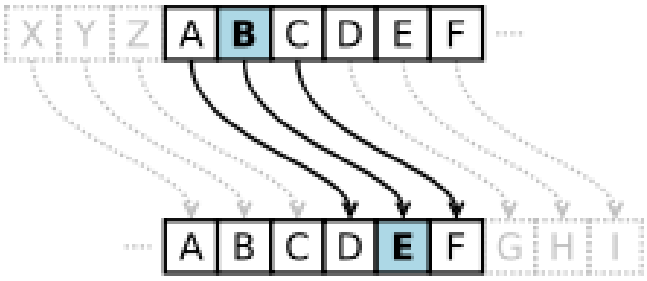
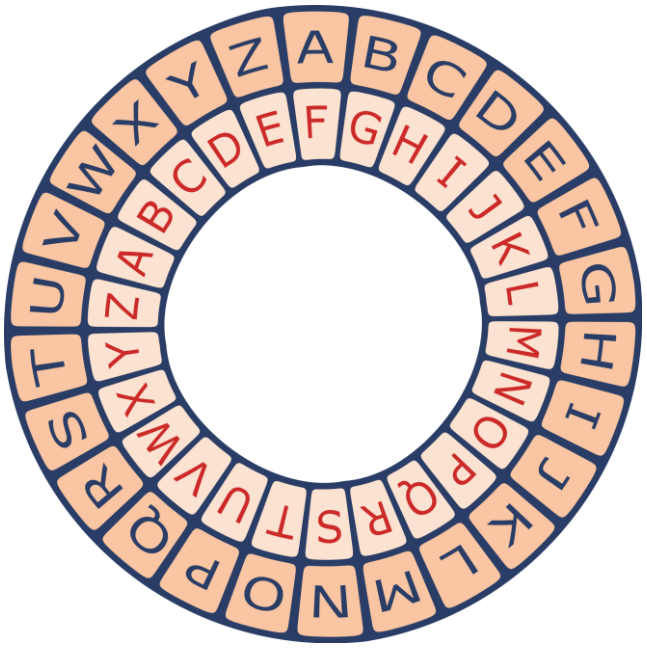
Der Cäsar-Algorithmus





Bei dem symmetrischen Verschlüsselungsverfahren der Cäsar-Verschlüsselung wird jeder Buchstabe des Klartextes aus einen Geheimbuchstaben abgebildet.

Die Zeichen werden zyklisch nach rechts verschoben(rotiert); zyklisch bedeutet, dass man beim Verschieben über Z hinaus wieder bei A anfangend weiterzählt. Die Anzahl der verschobenen Zeichen bildet **den Schlüssel**, der für die gesamte Verschlüsselung unverändert bleibt. Beispiel für eine Verschiebung um drei Zeichen:

```
Klar:    a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheim:  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Aus dem Klartext: "C Sharp" wird somit der Geheimtext "F VKDUS"

Algorithmus

Die Verschlüsselung in den verschlüsselten Buchstaben **C** eines Klarbuchstabens **P** mit einer Verschiebung um **K** Zeichen und einem Alphabet mit 26 Zeichen ist definiert als:

$$C = (P + K) \bmod 26$$

```
private static char Encrypt(char P,int K)
 {
     return (char)(P + K % 26);
 }
```

Entsprechend dazu lautet die Entschlüsselung eines Geheimbuchstabens C:

$$P = (C - K) \bmod 26$$

```
private static char Decrypt(char C, int K)
 {
     return (char)(C - K % 26);
 }
```