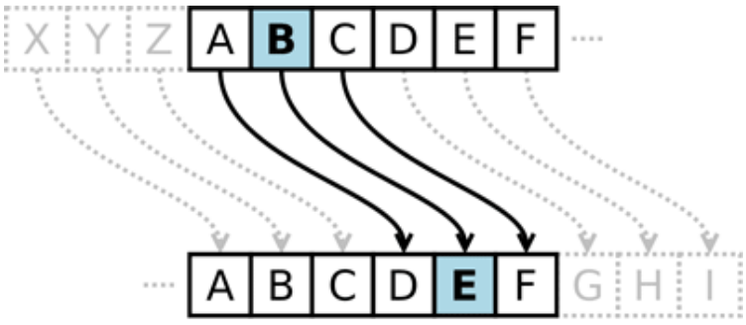
Die Cäsar-Verschlüsselung ist eine der ältesten Verschlüsselungsmethoden. Sie ist benannt nach Julius Cäsar. Cäsar erfand die Verschlüsselung, da er einen Weg brauchte um geheime Nachrichten an seine Feldherren zu schicken ohne dass Feinde diese mitlesen konnten.

So funktioniert die Cäsar-Verschlüsselung:
Jeder Buchstabe deiner geheimen Nachricht wird um eine bestimmte Anzahl Buchstaben entlang des Alphabets verschoben und ersetzt. So kann man zum Beispiel entscheiden, dass aus jedem A ein D wird. Dann wird aus jedem B ein E, aus jedem C ein F und so weiter. Aus dem Z wird dann ein C.



Der Buchstabe mit dem du das A ersetzen willst, wird Schlüssel genannt. Diesen braucht man auch um den Text wieder zu entschlüsseln und das Alphabet zurück zu schieben.

Beispiel:
Der Satz “ich bin der cryptocroc” mit dem Schlüssel Q wird zu “ysx ryd tuh shofjeshes”

Wie sicher ist die Cäsar-Verschlüsselung?
Sie ist nicht sicher, da es nur 25 Möglichkeiten gibt eine Nachricht zu kodieren. So kann das Verfahren zum Beispiel durch ausprobieren oder eine Häufigkeitsanalyse sehr leicht geknackt werden.