



Cäsar-Verschlüsselung

Was ist die Cäsar-Verschlüsselung?

Die Caesar-Scheibe ist eine einfache Verschlüsselungsmethode aus der Antike, die vom römischen Kaiser Julius Caesar verwendet wurde. Sie basiert auf der Idee, jeden Buchstaben im Alphabet um eine feste Anzahl von Positionen zu verschieben. Diese Anzahl nennt man den Schlüssel.

Beispiel:

Wenn die Verschiebung 3 ist, wird aus „A“ ein „D“, aus „B“ ein „E“ und so weiter. Das Alphabet „rotiert“ also um 3 Positionen.

Die Cäsar Scheibe

Zum Verschlüsseln und Entschlüsseln nutzen wir eine sogenannte Cäsar Scheibe. Sie besteht aus einem inneren und einem äußeren Ring. Die innere (bunte) Scheibe kann gedreht werden. Damit stellt man ein, wie weit das Alphabet verschoben wird.

Man dreht die innere bunte Scheibe so oft wie es der Schlüssel angibt. Danach verändern wir die Drehung nicht mehr.

Zum Verschlüsseln sucht man den Buchstaben auf dem äußeren Ring (Klartextalphabet) und ersetzt ihn mit dem Buchstaben (Geheimtextalphabet) untendrunter.

Zum Entschlüsseln sucht man den Buchstaben im inneren Ring (Geheimtextalphabet) und ersetzt ihn durch den oben drüber (Klartextalphabet).

