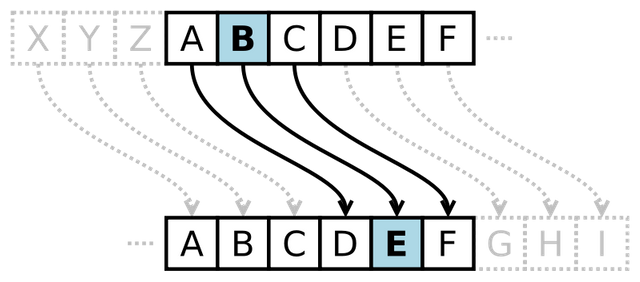
Caesar-Verschlüsselung

Die Caesar-Verschlüsselung ist eine der ältesten bekannten Verschlüsselungsmethoden. Sie ist jedoch sehr unsicher und kann sogar ohne Computerunterstützung schnell geknackt werden.

**Vorgehen zum Verschlüsseln**

Bei der Caesar-Verschlüsselung wird jeder Buchstabe der Nachricht um eine bestimmte Zahl im Alphabet weitergeschoben. Diese Zahl ist der geheime Schlüssel.

Wählt man zum Beispiel den Schlüssel **3**, so wird aus einem **A** (1. Buchstabe im Alphabet) ein **D** (4. Buchstabe), aus einem **B**ein **E**, aus einem **C** ein **F** usw.

Gelangt man bei der Verschiebung über Z hinaus, so wird wieder bei A begonnen. Also wird in dem Beispiel mit dem Schlüssel 3 das **X** durch **A**, **Y** durch **B** und **Z** durch **C** ersetzt.

**Beispiel**

Als Beispiel soll der Text "Mein Vater erklärt mir jeden Sonntag unseren Nachthimmel" mit dem Schlüssel **7** verschlüsselt werden

Man kann zuerst eine Tabelle erstellen, damit man die Buchstaben direkt ablesen kann:

Klartext: 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: H I J K L M N O P Q R S T U V W X Y Z A B C D E F G

Nun ersetzt man die Buchstaben entsprechend der Tabelle, also das M durch T, das E durch L usw.

Der Geheimtext ist somit: **TLPU CHALY LYRSHLYA TPY QLKLU ZVUUAHN BUZLYLU UHJOAOPTTLS** (Die Leerzeichen werden normalerweise entfernt, um die Sicherheit zu erhöhen)

**Vorgehen zum Entschlüsseln**

Zum Entschlüsseln verwendet man den geheimen Schlüssel und verschiebt alle Buchstaben im Geheimtext um diese Zahl im Alphabet zurück.