# Caesar-Verschlüsselung

Die Caesar-Verschlüsselung ist eine der ältesten und einfachsten Verschlüsselungsmethoden für Geheimtexte. Der Name geht auf den römischen Feldherren Julius Caesar zurück, der laut Überlieferungen diese Methode verwendete, um seine geheimen Botschaften für Außenstehende unkenntlich zu machen. Leider folgt die Verschlüsselung einem recht einfachen Prinzip und kann deshalb leicht von Unwissenden durchschaut werden. (Caesar hatte das Glück, dass nahezu niemand wusste wie seine Verschlüsselung funktioniert. Heute ist das aber nicht mehr so.) Wir zeigen dir aber noch ein paar Tricks und Kniffe, wie du sie etwas sicherer machen kannst.

## Grundlegendes Prinzip:

Bei dieser Verschlüsselungsmethode wird jeder Buchstabe durch einen anderen ersetzt, der sich durch eine Verschiebung des Alphabets ergibt. Wählt man also eine Verschiebung um drei Buchstaben, wird jedes A zu einem D, jedes B zu einem E, usw. Diese Verschiebung heißt auch Schlüssel und kann durch eine Zahl, in unserem Beispiel 3, oder als Buchstabe, in unserem Beispiel D, angegeben werden und muss dem Verfasser und dem Empfänger der Nachricht bekannt sein. Der Schlüssel kann auch innerhalb der Nachricht vermittelt werden, zum Beispiel durch den ersten oder letzten Buchstaben der Nachricht. Damit du nicht bei jedem Buchstaben wieder zählen musst, gibt es einen einfachen Trick. Zuerst schreibst du das Alphabet ganz normal hintereinander:

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Darunter schreibst du nun erneut das Alphabet. Nur, dass du es um die von dir festgelegte Anzahl (in unserem Beispiel also um 3 Stellen) zyklisch nach links verschiebst. Zyklisch heißt, dass du, wenn du bei Z angekommen bist, wieder mit A anfängst.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

Wenn du jetzt einen Text verschlüsseln willst, zum Beispiel „KRIMIS SIND TOLL“, suchst du jeden Buchstaben in der ersten Zeile und ersetzt ihn mit dem Buchstaben darunter. Der Beispielsatz würde mit unserer Verschlüsselung dann so aussehen: „NULPLV VLQG WROO“
Um einen verschlüsselten Text wieder lesbar zu machen, musst du zuerst den verwendeten Schlüssel kennen, also die Zahl, um die du das Alphabet verschieben musst. Dann schreibst du das verschobene Alphabet über das normale Alphabet.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

Zum Entschlüsseln suchst du nun jeden Buchstaben des verschlüsselten Textes in der oberen Zeile und ersetzt ihn durch den Buchstaben darunter. Probier‘s doch gleich mal mit der Tabelle oben und folgendem Text aus: „PHLVWHUGHWHNWLYH EHL GHU DUEHLW“.

## Varianten der Verschlüsselung:

ROT13: ROT13 bedeutet „rotate by 13 places“, also „rotiere um 13 Stellen“. Unser Schlüssel ist also die Verschiebung um 13 Stellen. Daraus würde sich folgende Tabelle ergeben:

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

Fällt dir an der Tabelle vielleicht etwas auf? Genau! Es stehen immer die zwei selben Buchstaben untereinander. Unter dem A steht nämlich ein N und unter dem N ein A. Dadurch hat diese Variante der Caesar-Verschlüsselung den Vorteil, dass man zum ver- und entschlüsseln dieselbe Tabelle verwenden kann, wodurch das Verfahren sehr schnell anzuwenden ist. Aber leider macht das die Methode noch ein bisschen unsicherer und ist mehr ein Rätsel als ein richtiger Geheimcode.

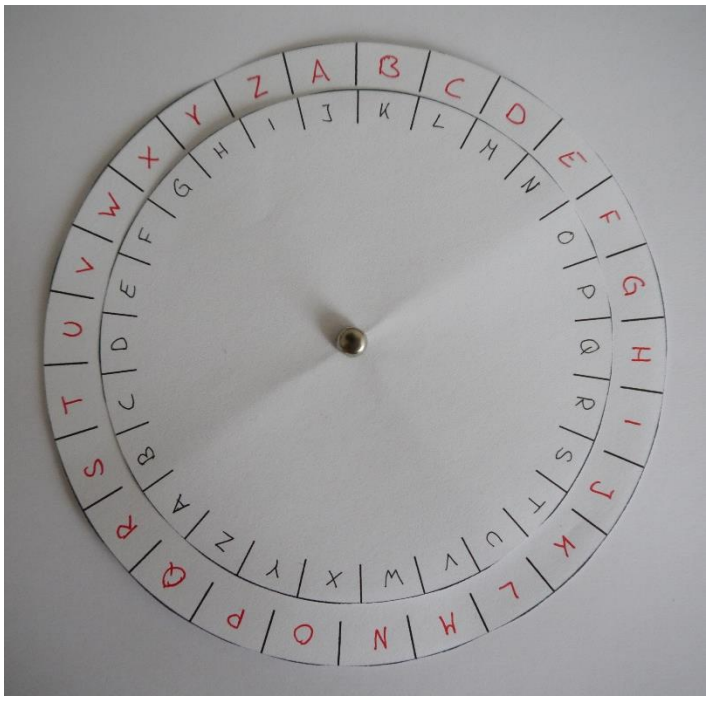
Atbasch: Diese Variante funktioniert ähnlich wie die ROT13 Methode. Sie beruht ursprünglich auf dem hebräischen Alphabet und ist auch eine sehr einfache Variante der Caesar-Verschlüsselung. Hierbei schreiben wir das Alphabet nämlich einfach rückwärts unter das normale Alphabet. Wir ersetzen also den ersten mit dem letzten Buchstaben, den zweiten mit dem vorletzten Buchstaben, usw. Daraus ergibt sich auch der Name dieser Methode, denn im hebräischen Schriftsystem ist der erste Buchstabe ein A, der mit dem letzten – ein T – vertauscht wird, und der zweite Buchstabe ein B, der mit dem vorletzten – ein Sch – vertauscht wird. Die Tabelle hierfür sieht so aus:

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

Wie du siehst, stehen auch hier wieder die zwei selben Buchstaben untereinander, wodurch diese Variante auch eher als Rätsel und nicht als Geheimcode anzusehen ist.

## Chiffrierscheibe:

Wenn du die Caesar-Verschlüsselung öfter anwenden möchtest, kannst du dir auch eine Chiffrierscheibe basteln. Damit du dir nicht immer eine Tabelle zeichnen musst. Hierfür brauchst du zwei unterschiedlich große, runde Scheiben. Auf beide schreibst du am Rand das Alphabet, wenn du möchtest sogar in zwei unterschiedlichen Farben. Nachdem du sie ausgeschnitten hast, befestigst du die kleinere der beiden Scheiben so auf der größeren, dass du sie drehen kannst. Das funktioniert zum Beispiel mit einer Musterbeutelklammer. Nun kannst du die Kleinere je nach gewähltem Schlüssel so verdrehen, dass du die Verschlüsselung ganz einfach ablesen kannst. Die größere Scheibe zeigt hierbei den Buchstaben deines ursprünglichen Textes, die kleiner Scheibe ist der verschlüsselte Buchstabe. Zum Entschlüsseln stellst du die Scheiben wieder richtig ein, suchst den Buchstaben des verschlüsselten Textes auf der inneren Scheibe und liest den richtigen Buchstaben auf der äußeren Scheibe ab.



## Tipps für mehr Sicherheit:

Um diese einfache Verschlüsselung doch etwas sicherer zu machen, gibt es ein paar Tricks, die du anwenden kannst.
Wir haben in unserem Beispiel nur mit Großbuchstaben gearbeitet, du kannst aber Groß- und Kleinbuchstaben verwenden und jeweils einen anderen Schlüssel einsetzen. Also zum Beispiel alle Großbuchstaben mit einer Verschiebung um 5 und alle Kleinbuchstaben mit einer Verschiebung um 18 codieren.
Oder du verwendest Großbuchstaben oder Zahlen, um innerhalb des Textes eine neue Verschiebung anzuzeigen. Nehmen wir wieder unser Beispiel „Krimis sind toll“ könnte man hier jeden Anfangsbuchstaben eines Wortes großschreiben und dies als Hinweis für den Schlüssel verwenden. Wichtig ist hier aber, dass man den Anfangsbuchstaben nicht mit verschlüsselt, damit der Empfänger der Nachricht weiß, wie er die Worte entschlüsseln kann. Verschlüsselt sähe unser Beispieltext dann so aus: „Kbswsc Safv Thee“
Eine weitere Möglichkeit besteht darin, nicht nur die 26 Buchstaben des Alphabets für die Verschlüsselung zu verwenden, sondern auch Zahlen oder Sonderzeichen, wie Kommas, Ausrufezeichen oder Fragezeichen in die Tabelle oder auf deine Chiffrierscheibe einzutragen.
Oder du ordnest das Alphabet nicht in der richtigen Reihenfolge, sondern zufällig an. Eine Tabelle mit der Verschiebung um 3, bei der die obere Zeile zufällig angeordnet wurde (natürlich kannst du auch die untere Zeile zufällig ordnen), könnte dann so aussehen:

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

Bei dieser Variante ist die vorherige Absprache zwischen Verfasser und Empfänger jedoch absolut erforderlich, damit der Empfänger die Nachricht auch entziffern kann.
Außerdem empfiehlt es sich am Anfang noch einige zufällige Buchstaben mit in die Nachricht einzubauen. Sollte nämlich doch einmal ein Fremder die Botschaft in die Hände bekommen, wird er wahrscheinlich versuchen, das erste Wort herauszufinden. Hast du hier jedoch einfach irgendwelche Buchstaben notiert, kann er keine sinnvolle Nachricht herauslesen.