

# CAESER-CODE

Niklas von Hirschfeld

Gymnasium Lüneburger Heide

## Einleitung

Der **Caesercode** (auch Caesar-Verschlüsselung oder -Verschiebung) ist ein *symmetrisches*<sup>1</sup> Verschlüsselungsverfahren, welches nach Julius Caesar benannt ist. Dieser habe es für die Kommunikation mit seinen militärischen Verbündeten genutzt. Nachrichten mussten über lange Distanzen transportiert werden. Dabei passierte es nicht selten, dass solche Nachrichten abgefangen wurden. Damit dabei keine vertraulichen Informationen an den *Gegner* gerieten, wurde die Caesar-Verschlüsselung genutzt.

## Vorteile

Damals war dieses Verschlüsselungsverfahren gut und effektiv. Der größte Vorteil war zu der damaligen Zeit die **Unbekanntheit**. Wenn ein solches Verfahren noch nicht bekannt oder verbreitet ist, gibt es weniger Ansetze und Interesse es zu knacken. Ein weiterer Vorteil ist die **schnelle Ver- und Entschlüsselung**, wodurch die Information schnell Menschen lesbar gemacht und genutzt werden können.

## Sicherheit

Schlüsseln ist ein Lösen des Codes mit demselben Schlüssel, wie auch Verschlüsseln. Mittlerweile gilt dieses Verfahren als **nicht sicher**.<sup>2</sup> Durch ihre begrenzte Anzahl an

realistisch.

Da dieses Verfahren schon alt und auch relativ einfach ist, gibt es mittlerweile viele gute und schnelle Wege, den Code zu lösen. Die gängigsten sind eine **Bruteforce-Attacke** oder eine **Häufigkeitsanalyse**.

<sup>1</sup> Mittlerweile gilt dieses Verfahren als nicht sicher.  
<sup>2</sup> Ausprobieren von allen möglichen Schlüsseln

# CAESER-CODE

Niklas von Hirschfeld

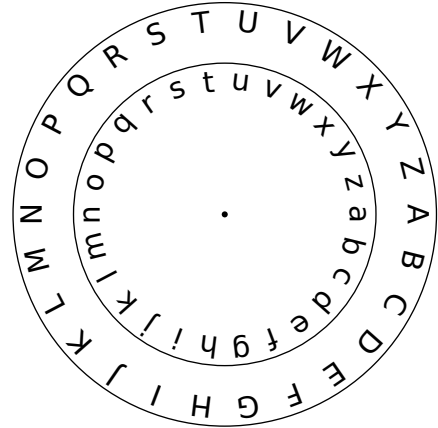
Gymnasium Lüneburger Heide

Beim **Brutforce** werden einfach **alle** möglichen Schlüssel ausprobiert. Bei aktuellen und herkömmlichen Verschlüsselungsmethoden dauert diese Attacke in der Theorie oft mehrere Jahrzehnte, auch mit den aktuellsten Computern. Beim Caesar-Verfahren sollte es allerdings nicht länger als Minuten oder sogar Sekunden dauern, da die Anzahl an möglichen Schlüsseln bei 26 liegt. Zwar ist auch ein Schlüssel wie 27 *möglich* allerdings funktioniert dieser exakt wie der Schlüssel 1.

Bei der **Häufigkeitsanalyse** geht es darum, die Anzahl der auftauchenden Buchstaben zu analysieren. Diese vergleicht man dann mit der Häufigkeit des jeweiligen Buchstaben in der Ziel Sprache generell. Im Deutschen ist der am häufigsten auftauchende Buchstabe das *e*. Wenn jetzt ein Buchstabe am häufigsten auftaucht, ist es mit hoher Wahrscheinlichkeit das verschlüsselte *e*.

## Tools

Den Prozess des Codieren können verschiedene Werkzeuge oder auch Skripte vereinfachen und verschnellern. Hier abgebildet ist Papierkonstrukt, bestehend aus einer großen und einer kleineren Scheibe.



Die Buchstaben sind nach dem Alphabet angeordnet und somit kann die innere Scheibe weitergedreht werden, um einen neuen Schlüssel darzustellen.