CAESER-CODE

Niklas von Hirschfeld

Gymnasium Lüneburger Heide

Einleitung

Der **Caesercode** (auch Caeser-Verschlüsselung oder -Verschiebung) ist ein *symmetrisches*[1] 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 Caeser-Verschlüsselung genutzt.

Vorteile

Damals war dieses Verschlüsselungsmethode gut und effektiv. Die größte Vorteil war zu der darmaliegen Zeit die **Unbekanntheit**. Wenn ein solches Verfahren noch nicht bekannt oder Verbreitet ist, gibt es weniger ansetze und intresse es zu knacken. Ein weiter Vorteil ist die **schnelle Ver- und Entschlüsselung**, wodurch die Infomation schnell Menschenlesbar gemacht und genutzt werden können.

Sicherheit

Schlüsseln, ist ein lösen des Codes mit Hilfe der *Bruteforcemethode*[2] deutlich **Sicher**. Durch ihre begrenzte Anzahl an

Mittlerweile gilt dieses Verfahren als **nicht**

realistisch.

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

[1] es wird sowohl für die Ver- wie auch Entschlüsselung der selbe Schlüssel verwendet.

[2] Ausprobieren von allen möglichen Schlüsseln

CAESER-CODE

Niklas von Hirschfeld

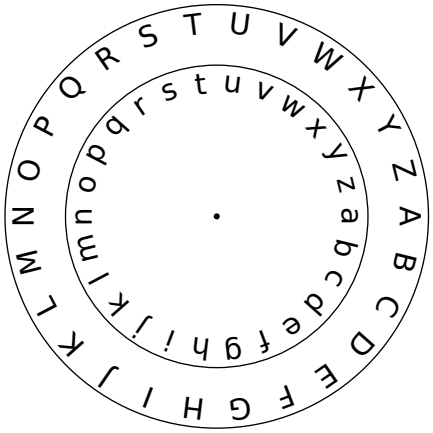
Gymnasium Lüneburger Heide

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 Caeser-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 jeweiliegen Buchstaben in der ziel Sprache generell. Im deutschen ist der am häufigsten auftauchnde 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 Scripte vereinfach 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 inner Scheibe weitergedreht werden, um eine neuen Schlüssel darzustellen.