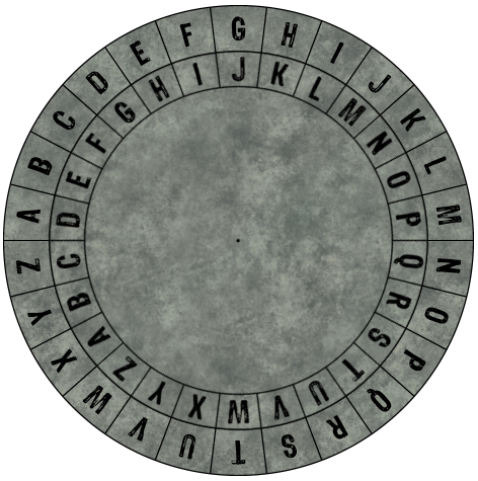
# EduBreakout: Was ist Informatik?

## Regionalverband Saarbrücken: Caesar-Chiffre

Schon lange verwenden Menschen Verschlüsselungsverfahren, um geheime Informationen miteinander zu teilen. Eines der bekanntesten Verfahren wurde von dem römischen Feldherren Julius Caesar zur militärischen Kommunikation verwendet und nach ihm benannt: die Caesar-Chiffre. Bei der Caesar-Chiffre werden die Buchstaben des Textes durch andere Buchstaben ersetzt (substituiert), die im Alphabet um eine bestimmte Anzahl von Stellen weiter hinten stehen. Man kann dazu eine Caesar-Scheibe verwenden, die man durch Drehen auf einen bestimmten Startbuchstaben (den sogenannten Schlüssel) einstellt, oder eine Tabelle anlegen.



„Caesar-Scheibe“ von Stefan Hanauska; CC BY-SA; https://creativecommons.org/licenses/by-sa/4.0/deed.de; https://hanauska.info/tools/caesar/caesar.html

| original | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| verschlüsselt | 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 |

Beim Verschlüsseln mit der Tabelle sucht man die Buchstaben des Textes in der oberen Zeile und ersetzt sie durch den jeweils darunter stehenden Buchstaben. Ein `H` wird so umgewandelt in ein `K`, ein `A` in ein `D` usw. So wird aus dem Wort `HALLO` mit Hilfe der oberen Tabelle `KDOOR`.

Wenn man einen geheimen Text erhält und diesen entschlüsseln möchte, sucht man die Buchstaben hingegen in der unteren Zeile und ersetzt sie durch den jeweils darüber stehenden Buchstaben. So kann man den Geheimtext `VDDUODQG` wieder lesbar machen als `SAARLAND`.

Nun bist du gefordert:
Vervollständige zunächst die Tabelle, indem du die Buchstaben in alphabetischer Reihenfolge einträgst. Nachdem du den letzten Buchstaben des Alphabetes notiert hast, beginnst du mit dem Alphabet von vorne. Hier lautet der Schlüssel „I“.

| original | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| verschlüsselt | I | J | K | | | | | | | | | | | | | | | | A | | | | | | | |

Entschlüssele anschließend den folgenden Geheimtext anhand der von dir ergänzten Tabelle, um deinen dritten Zahlencode zu erhalten:

`V M C V M Q V A A Q M J M V`

Lösung: _____

Da man die Caesar-Scheibe nur auf 25 verschiedene Arten einstellen kann, ist es natürlich nicht besonders schwer, einen auf diese Art verschlüsselten Text lesbar zu machen – auch wenn man den Text abgefangen hat und den Schlüssel gar nicht kennt. Man muss nur alle 25 Schlüssel ausprobieren. Deshalb nutzt dieses Verfahren heute natürlich niemand mehr, der Informationen geheim halten möchte.

Moderne Verfahren beruhen meist auf komplexen mathematischen Berechnungen, deren Umkehrung nicht so einfach möglich ist wie bei der Caesar-Chiffre.