# Monoalphabetische Verschlüsselung

## *Aufgaben:*

4. *Beschreibe, was bei diesem Verfahren der Schlüssel ist.*
   *Lösung: Der Schlüssel besteht sowohl aus der Verteilung der Buchstaben auf der Scheibe, als auch aus der Einstellung der Scheibe. Jede Scheibeneinstellung könnte mit einer anderen Verteilung der Buchstaben realisiert werden. Daher ist eigentlich nur die Verteilung der Buchstaben wichtig.*
5. *(*) Wie viele verschiedene Schlüssel sind möglich?*
   *Lösung: Für den ersten Buchstaben hat man 26 Möglichkeiten, für den zweiten 25 usw. Daraus ergibt sich 26*25*24*23...*2*1 = 26! = 400 Quadrillionen*

### Brechen der Verschlüsselung

Es ist nicht mehr möglich, alle Schlüssel durchzuprobieren (Brute Force-Verfahren).

6. *Begründe, warum die Häufigkeitsanalyse immer noch eine Angriffsmöglichkeit bietet.*
   *Lösung: Jedem Buchstaben wird genau ein anderer zugeordnet. Damit sticht z.B. das E immer noch heraus.*
7. 

VCS YPAPKFTUKESZCBNUS BIEBZCZIZCPA CBZ SCAS DSQESBBSQIAG VSB NKSBKQ-KFGPQCZUYIB, VK SB YSUQ YPSGFCNUS BNUFISBBSF GCEZ. FSCVSQ HKAA YKA YCZ VSQ UKSIMCGHSCZBKAKFWBS CYYSQ APNU VSA HFKQZSJZ SQYCZZSFA. YKA UKZ KESQ KINU UCSQMISQ XSCZSQSAZXCNHFIAGSA, VCS VI HSAASAFSQABZ, XSAA VI XSCZSQ CAMPQYKZCH CA VSQ BNUIFS YKNUBZ. SB GCEZ R.E. VCS DCGSASQS-DSQBNUFISBBSFIAG, VKB KIZPHSW-DSQMKUQSA PVSQ VKB PAS-ZCYS TKV. VKB FSZRZS DSQMKUQSA CBZ RXKQ IATQKHZCBNU, KESQ ECSZSZ TSQMSHZS BCNUSQUSCZ. SB XIQVS R.E. MISQ VCS KEBCNUSQIAG VSQ HPYYIACHKZCPA RXCBNUSA KYSQCHKACBNUSA TQKSBCVSAZSA IAV QIBBCBNUSA TQKSBCVSAZSA DSQXSAVSZ.

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

DIE MONOALPHABETISCHE SUBSTITUTION IST EINE VERBESSERUNG DES CAESAR-ALGORITHMUS, DA ES MEHR MOEGLICHE SCHLUESSEL GIBT. LEIDER KANN MAN MIT DER HAEUFIGKEITSANALYSE IMMER NOCH DEN KLARTEXT ERMITTELN. MAN HAT ABER AUCH HIERFUER WEITERENTWICKLUNGEN, DIE DU KENNENLERNST, WENN DU WEITER INFORMATIK IN DER SCHULE MACHST. ES GIBT Z.B. DIE VIGENERE-VERSCHLUESSELUNG, DAS AUTOKEY-VERFAHREN ODER DAS ONE-TIME PAD. DAS LETZTE VERFAHREN IST ZWAR UNPRAKTISCH, ABER BIETET PERFEKTE SICHERHEIT. ES WURDE Z.B. FUER DIE ABSICHERUNG DER KOMMUNIKATION ZWISCHEN AMERIKANISCHEN PRAESIDENTEN UND RUSSISCHEN PRAESIDENTEN VERWENDET.