

## Monoalphabetische Substitution

Monoalphabetische Substitution ist der Fachbegriff für ein Ersetzungsverfahren, das jedem **Klartextzeichen** genau ein **Geheimtextzeichen** zuordnet. Das Caesar-Verfahren ist ein Beispiel für eine solche Ersetzung. Anstatt das Alphabet zu verschieben, können die Geheimtextzeichen den Klartextzeichen aber auch beliebig zugeordnet werden. Eine Zuordnungstabelle könnte zum Beispiel so aussehen:

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

Tabelle 1: Beispiel für eine monoalphabetische Verschlüsselung

### Aufgabe 1:

- a) Verschlüssele den Text *morgen schuelerstreich* mithilfe der Tabelle 1.

\_\_\_\_\_

- b) Entschlüssele den Text MWXV RGX WI mithilfe der Tabelle 1.

\_\_\_\_\_

### Aufgabe 2:

- a) Erstelle dir mit deinem Nachbarn/deiner Nachbarin eine Zuordnungstabelle für eine monoalphabetische Substitution. Als Geheimtextzeichen könnt ihr nicht nur Buchstaben, sondern beliebige Zeichen, also z. B. auch Zahlen, Smileys usw. verwenden. Ihr benötigt aber 26 verschiedene Geheimtextzeichen. Warum?

Klartextzeichen	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
Geheimtextzeichen																										

- b) Tausche mit deinem Nachbarn geheime Nachrichten aus, die ihr mit eurer Zuordnungstabelle ver- und entschlüsselt.

verschlüsselte Nachricht: \_\_\_\_\_

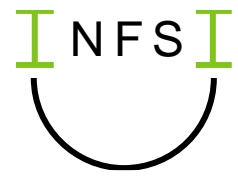
entschlüsselte Nachricht: \_\_\_\_\_

**Aufgabe 3:** Gib an, was bei einer monoalphabetischen Substitution die geheime Information ist, die als Schlüssel dient.

Schlüssel: \_\_\_\_\_

**Aufgabe 4:** Wenn man die Zuordnungstabelle nicht kennt, ist es auf den ersten Blick ziemlich schwierig den verschlüsselten Text zu lesen. Denn es würde ziemlich lange dauern, alle möglichen Zuordnungen auszuprobieren. Es gibt  $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot \dots \cdot 1 = 403.291.461.126.605.635.584.000.000$  Möglichkeiten. Das sind ungefähr 403 Trilliarden.

- a) Begründe, warum es bei der Verwendung einer Zuordnungstabelle, die den Klartextzeichen beliebige Geheimtextzeichen zuordnet, im Vergleich zum Caesar-Verfahren so viel mehr Möglichkeiten gibt, die ein Angreifer ausprobieren müsste.
- b) Sammelt Ideen für schnellere Ansätze, wie sich ein Text, der mit einer beliebigen Zuordnungstabelle verschlüsselt wurde, knacken lässt.



Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](https://creativecommons.org/licenses/by-nc-sa/4.0/). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.