

Monoalphabetische Substitution

Einfache monoalphabetische Substitutionsverfahren ordnen jedem Klartextzeichen genau ein Geheimtextzeichen zu. Eine solche Zuordnungstabelle könnte zum Beispiel so aussehen:

Klartext- zeichen	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
Geheimtext- zeichen	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 Ersetzungstabelle einer monoalphabetischen Substitution

Aufgabe:

- Verschlüsseln Sie den Text *angriff um zehn* mithilfe der Tabelle 1.
- Entschlüsseln Sie den Text MWXV RGX WI mithilfe der Tabelle 1.
- 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. Rechnen Sie aus, wie viele Möglichkeiten es gibt.
- Suchen Sie nach anderen Ansätzen zum Knacken monoalphabetisch verschlüsselter Texte.

