

Station C: Allgemeine Substitutionschiffre

Das nun vorgestellte Verfahren kann man als eine Verallgemeinerung der beiden vorherigen Verschlüsselungen auffassen. Die Buchstaben des Klartextalphabetes werden nämlich einfach "durcheinander gewürfelt" (man sagt: *permutiert*) und ergeben damit schon das Geheimtextalphabet. Ein Beispiel für eine solche Permutation, die völlig willkürlich ist, ist in der folgenden Tabelle dargestellt.

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

Beispiel 1 (Verschlüsselung): Der Klartext `permutation` wird mit obiger Tabelle in den Geheimtext `RGXOZQIQUKY` verschlüsselt.

Beispiel 2 (Entschlüsselung): Der (ebenfalls mit obiger Tabelle verschlüsselte) Geheimtext lautet: `CRICC`. Wir lesen den Klartext ab: `spass`.

Aufgabe 1: Gegeben ist folgende Tabelle:

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

Entschlüssele mit Hilfe dieser Tabelle den Geheimtext `WXMLKVLKRLA..`

Aufgabe 2: Was ist bei diesem Verfahren ein "Schlüssel"? Wie viele gibt es?

Aufgabe 3 (Zusatz): Verschlüssele mit der Tabelle aus Aufgabe 1 den Klartext `menetekel`. Vergleiche den Klartext und den Geheimtext. Was fällt auf?