

Station B: Verschlüsselung mit Schlüsselwort

Bei dieser Art der Verschlüsselung ist der Schlüssel keine Zahl (wie beim Cäsar-Verfahren), sondern ein Wort, das sogenannte **Schlüsselwort**. Als Beispiel betrachten wir das Wort FUEHRERSCHNEIN. Von diesem Wort streichen wir nun alle mehr als einmal vorkommenden Buchstaben. Es bleibt damit die Zeichenreihe FUEHRSCIN. Diese Zeichenreihe bestimmt die Verschlüsselung der ersten Buchstaben des Klartextalphabetes. Man ersetzt also a durch F, b durch U, c durch E, d durch H usw. Auf diese Weise hat man die ersten Buchstaben des Geheimentextalphabetes festgelegt (Hier sind es neun). Die restlichen Buchstaben werden anschließend in der umgekehrten Reihenfolge des Alphabets verschlüsselt, wobei man die Buchstaben des Schlüsselwortes auslässt. In unserem Beispiel erhalten wir also folgende Tabelle zum Verschlüsseln.

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

Beispiel 1 (Verschlüsselung): Der Klartext lautet: november. Wir verschlüsseln mit dem Schlüsselwort FUEHRERSCHNEIN. Nach obiger Tabelle erhält man den Geheimtext: VTJRWURO.

Beispiel 2 (Entschlüsselung): Der Geheimtext lautet: LWHXMNXMWK. Das Schlüsselwort ist bekannt und lautet: GEHEIM. Nach Streichung der mehrfach auftretenden Buchstaben dieses Wortes bleibt die Zeichenreihe GEHIM und man erhält 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	G	E	H	I	M	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	L	K	J	F	D	C	B	A

Liest man die Tabelle wieder "von unten nach oben", so erhält man den Klartext sicherheit.

Aufgabe 1: Verschlüssele den Klartext wintereinbruch mit dem Schlüsselwort HOHO. Entschlüssele den Geheimtext KPRMJRXHK mit dem Schlüsselwort REUTLINGEN. Stelle dazu jeweils die Tabelle zum Ver- und Entschlüsseln auf.

Aufgabe 2 (Zusatz): Entschlüssele den Geheimtext YDHJIXZVHXKMDSUBMH.