Vigenère-Chiffre

Die **Vigenère-Verschlüsselung** ist eine Erweiterung der Cäsar-Verschlüsselung. Der Unterschied besteht darin, dass man nun nicht eine fixe Verschiebung der Buchstaben hat, sondern sich diese bei jedem Buchstaben ändert. Man hat ein ganzes Wort als Schlüssel, dessen Buchstaben die jeweilige Verschiebung angeben.

Wie man im unteren Beispiel sieht, kann ein S einmal auf Z und einmal auf W abgebildet werden, dies hängt vom Schlüsselwort ab. Wenn das Schlüsselwort z.B. HEY ist, so wird der erste Buchstabe um 7, der zweite um 4, der dritte um 24 verschoben. Ist das Schlüsselwort kürzer als der zu verschlüsselnde Text, wird das Schlüsselwort noch einmal angeschrieben. Ist das Schlüsselwort länger, werden nur die ersten paar benötigten Buchstaben des Wortes verwendet.

Beispiel:

Klartext: SPASS

Schlüssel: HEY

Klartext	S	P	A	S	S
Schlüssel	***H***	***E***	***Y***	*H*	*E*
Geheimtext	Z	T	Y	Z	W

Es kann sehr aufwändig sein, bei jedem einzelnen Buchstaben die Verschiebung zu zählen und dann am Cäsar-Rad einzustellen, eine einfache Methode ist es, die **Hilfstabelle** auf der nächsten Seite zu verwenden. Dabei sucht man den zu verschlüsselnden Buchstaben (Klartext) in der obersten Zeile und den aktuellen Schlüsselbuchstaben in der ersten Spalte. Der Buchstabe, der zur betrachteten Zeile und Spalte gehört, ist der verschlüsselte Buchstabe (Geheimtext).

Beispiel:

Klartext: Informatikwerkstatt

Schlüssel: geheim

Klartext	I	N	F	O	R	M	A	T	I	K	W	E	R	K	S	T	A	T	T
Schlüssel	*G*	***E***	***H***	***E***	***I***	***M***	*G*	*E*	*H*	*E*	*I*	*M*	*G*	*E*	*H*	*E*	*I*	*M*	*G*
Geheimtext	O	R	M	S	Z	Y	G	X	P	O	E	Q	X	O	Z	X	I	F	Z