Strom-Chiffre

Substitution (polyalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Bei einer Stromverschlüsselung benötigt man einen Startschlüssel. Aus dem Startschlüssel entsteht zusammen mit dem Klartext ein Schlüsselstrom. Das heißt eine Reihe von Schlüsseln, wovon wir uns aber nur den Startschlüssel merken müssen.
Wir betrachten den speziellen Fall der Autokey-Verschlüsselung. Diese wurde, wie die Vigenère-Verschlüsselung, vom Franzosen Blaise de Vigenère (1523 bis 1596, s. Bild) entwickelt. Bei der Autokey-Verschlüsselung wird an den Startschlüssel der Klartext gehangen. Also werden die einzelnen Buchstaben zum Schlüssel für folgende Buchstaben.

Hinweis: Solltest du die Vigenère-Station noch nicht bearbeitet haben, macht es Sinn, dies zuerst zu tun, damit du Verbindungen ziehen kannst. Ansonsten wirst du das erste Beispiel nicht verstehen, kannst diese Station aber trotzdem weiter bearbeiten.

Beispiel Mit dem Schlüssel **GEHEIM** können wir die Nachricht mit dem Vigenère-Quadrat verschlüsseln. Dafür verschlüsseln wir die ersten Buchstaben mit dem Schlüsselwort und die folgenden Buchstaben mit dem Klartext von Anfang an.

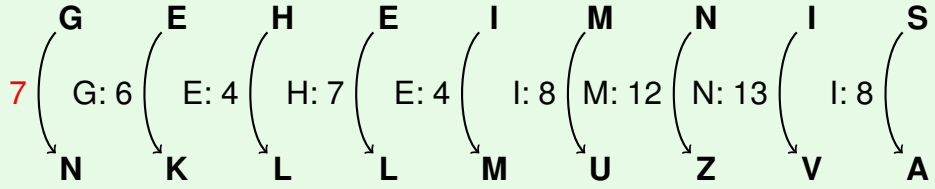
Nachricht:	DAS TREFFEN IST UM ACHT UHR
Schlüsselwort:	GEH EIMDAST REF FE NIST UMA
Geheimtext:	JEZ XZQIFWG ZWY ZQ NKZM OTR

Da wir das Arbeiten mit dem Vigenère-Quadrat jedoch bereits bei der Vigenère-Station gelernt haben, schauen wir uns eine weitere Möglichkeit für die Ver- und Entschlüsselung an. In der Wissenschaft wird häufig mit Zahlen anstatt mit Buchstaben gearbeitet. Dies vereinfacht vor allem die Arbeit mit Informatiksystemen. Außerdem veranschaulicht es besser, wieso die Autokey-Verschlüsselung als Stromverschlüsselung bezeichnet wird. Als Hilfsmittel verwenden wir den Stromverschlüsseler. Dieser zeigt dir die Stellen der einzelnen Buchstaben im Alphabet. Dabei fangen wir immer bei 0 an zu zählen. Deswegen wird der Buchstabe **A** mit der Stelle **0** gleichgesetzt.

Strom-Chiffre

Substitution (polyalphabetisch)

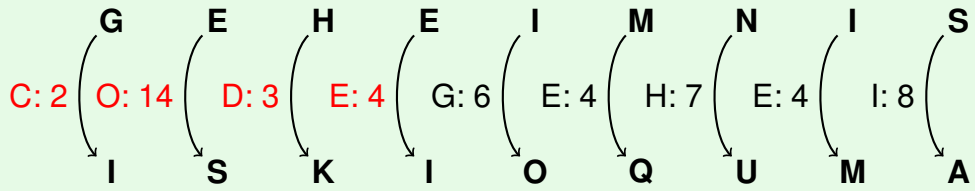
Beispiel Als Startschlüssel ist die Zahl **7** gewählt und unsere Nachricht lautet **GEHEIMNIS**. Nun stellen wir die Nachricht in den Stromverschlüsseler ein, indem wir die Buchstabenbänder so drehen, dass die Buchstaben in den ausgeschnittenen Fenstern unserer Nachricht entsprechen. Wir fangen von vorne an, die Buchstabenbänder jeweils um den passenden Schlüssel weiter zu drehen. Wir schieben also den ersten Buchstaben **G** 7 Stellen weiter und erhalten ein **N**. Dann schieben wir den zweiten Buchstaben **E** um die Stelle vom ersten Klartext weiter, also 6 Stellen, da G an der sechsten Stelle im Alphabet liegt, und landen bei **K**. Nun nehmen wir uns den dritten Buchstaben und schieben ihn um die Stelle vom zweiten Klarbuchstaben weiter. Dies machen wir so lange, bis wir alle Buchstaben verschlüsselt haben.



Unser Geheimtext lautet somit **NKLLMUZVA**.

Die »normale« Autokey-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Startschlüssel aus mehren Zahlen kombiniert wird. Um sich den Startschlüssel einfacher merken zu können, kann man auch ein Schlüsselwort wählen. Die Buchstaben des Schlüsselwortes werden wieder in Zahlen umgewandelt.

Beispiel Unser Startschlüssel ist jetzt **CODE**, was den Zahlen **2 14 3 4** entspricht, und unsere Nachricht lautet wieder **GEHEIMNIS**. Dann stellen wir die Nachricht in den Stromverschlüsseler ein und verschlüsseln zuerst die ersten vier Buchstaben mit unserem Schlüsselwort und die folgenden wie eben mit den Klartextbuchstaben der Nachricht von Anfang an.



Unser Geheimtext lautet also **ISKIOQUMA**.