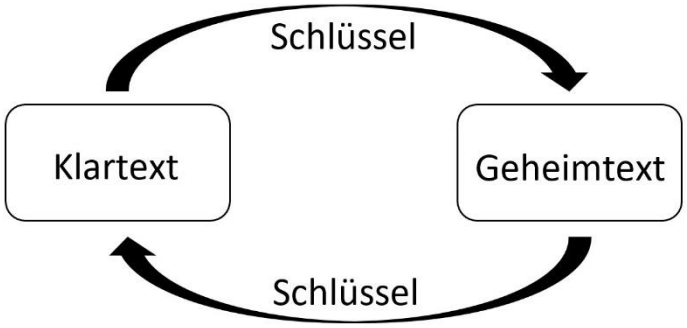
Wie funktionieren Geheimcodes eigentlich?

Texte, die gar keinen Sinn ergeben, wild angeordnete Buchstaben oder fremde Zeichen in einer scheinbar zufälligen Abfolge – so wirken Geheimcodes auf einen, wenn man sie nicht kennt und nicht entziffern kann. Aber eigentlich folgen alle Geheimcodes einem ähnlichen Prinzip, das wir dir hier erklären möchten. Grundlegend unterscheidet man zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Das klingt erst einmal wahnsinnig kompliziert, ist es aber eigentlich gar nicht.

Symmetrische Verschlüsselung

Alle Geheimschriften, die wir dir auf dieser Webseite erklären, sind symmetrische Verfahren. Die funktionieren so: Ein Text, auch Klartext genannt, wird durch einen Schlüssel verschlüsselt, wodurch der Geheimtext entsteht. Dieser wird vom Empfänger mit demselben Schlüssel wieder entschlüsselt.



Mit einem Gedankenexperiment ist das einfacher zu verstehen. Du möchtest deiner besten Freundin oder deinem besten Freund einen Brief schreiben, aber niemand außer euch soll ihn lesen können. Dafür hast du dir etwas ausgedacht. Du kaufst eine Schachtel, die man mit einem Schloss verschließen kann. Zu dem Schloss gibt es zwei Schlüssel: Einen behältst du, den anderen gibst du weiter an deine*n Freund*in. Als nächstes schreibst du einen Brief (den Klartext), legst ihn in die Schachtel mit dem Schloss und verschließt diese. Der Text ist nun also verschlüsselt. Entschlüsselt werden kann er nur durch den Schlüssel zu dem Schloss, den du ja weitergegeben hast.

Asymmetrische Verschlüsselung

Asymmetrische Verfahren sind wesentlich komplizierter. Sie werden als komplexen Algorithmen von Computern berechnet. Für alle, die trotzdem interessiert, wie es funktioniert, haben wir ein weiteres Gedankenexperiment.
Bei einer asymmetrischen Verschlüsselung wird der Schlüssel in zwei Teile geteilt. Der eine wird öffentlicher Teil genannt und ist jedem, der Interesse daran hat, zugänglich. Der andere Part wird privater Teil genannt und bleibt geheim.

Stellen wir uns wieder vor, du möchtest mit deiner besten Freundin oder deinem besten Freund Nachrichten austauschen, die nur ihr und kein anderer lesen soll. Du kaufst wieder eine Schachtel, die man mit einem Schloss verschließen kann. Dieses Mal besitzt aber jeder ein eigenes Schloss mit einem eigenen Schlüssel. Das Schloss ist der öffentliche Teil des Schlüssels, du gibst es deiner Freundin bzw. deinem Freund. Der Schlüssel zu diesem Schloss ist der private Teil, diesen behältst du und gibst ihn unter keinen Umständen an eine andere Person weiter. Möchte dein bester Freund bzw. deine beste Freundin dir nun eine Nachricht schicken, legt diese*r den Brief in die Schachtel und verschließt sie mit dem Schloss, das sie/er von dir bekommen hat. Da nur du den Schlüssel zu diesem Schloss besitzt, kannst nur du die Nachricht öffnen. Möchtest du nun auf den Brief antworten, verschließt du die Schachtel mit dem Schloss, das du von deiner Freundin bzw. deinem Freund bekommen hast. Nun kann die Box nur durch den zweiten Schlüssel geöffnet werden.