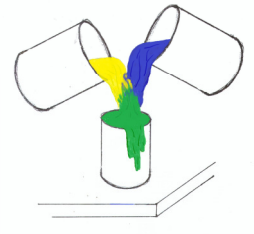
Einweg- und Falltürfunktionen

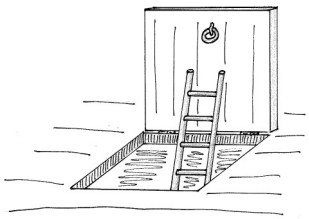
Begriffsklärung: Als *Einwegfunktion* bezeichnet man einen Vorgang, der in der einen Richtung sehr schnell und einfach auszuführen ist, der jedoch zumindest sehr schwer wenn nicht unmöglich rückgängig zu machen ist.

Einwegfunktionen sind in der Kryptologie grundlegend: Die Verschlüsselung einer Nachricht soll sehr schnell und einfach erfolgen, die Entschlüsselung (also in diesem Sinne das *eindeutige* „Rückgängig-machen" der Verschlüsselung) durch einen Hacker jedoch sehr schwer, wenn nicht gar unmöglich sein. Das Auffinden solcher Funktionen gilt als mit die größte Leistung der Kryptologen.



Ein Beispiel:

Wir mischen zwei Farben, z.B. „gelb" und „blau". Dabei erhält man „grün". Erläutere, warum das Mischen der zwei Farben eine Einwegfunktion darstellt. Vergleiche das Farbenbeispiel mit unserer Primzahlsituation beim Verschlüsseln durch Multiplikation.



Für die Anwendung in der Kryptologie ist also nun zunächst eine Einwegfunktion vonnöten. Diese muss jedoch noch eine weitere Anforderung erfüllen: Der berechtigte Adressat soll die Nachricht ja auch wieder entschlüsseln können. Es muss also für berechtigte Personen (mit Zusatzinformationen) eine Möglichkeit geben, die Verschlüsselung schnell rückgängig zu machen. Diesen Vorgang bezeichnet man als „Falltürfunktion".

1. *Recherchiere: gibt es (z.B. im Bereich der Chemie) für das Farbenbeispiel oben Falltürfunktionen?*
2. *Eine weitere Einwegfunktion mechanischer Art kennst du auch aus dem täglichen Leben. Ein Tipp: du erlebst sie, wenn du einen Papierbrief verschickst. Kommst du darauf? Gibt es auch hier eine Falltürfunktion?*
3. *Suche nach weiteren mehr oder weniger alltägliche Einwegfunktionen. Untersuche, ob es dafür Falltürfunktionen gibt. Tausche dich mit deinen KlassenkameradInnen aus!*