# Das RSA Verfahren

Um die Funktionsweise des RSA Verfahrens nachzuvollziehen, musst du dir Klartext, Geheimtext und Schlüssel nicht als Bit-Folgen wie bei AES, sondern einfach als natürliche Zahlen vorstellen. Für den Computer macht das sowieso keinen Unterschied, da dieser alle Daten als Bit-Folge abspeichert udn verarbeitet.

## Einwegfunktionen und Falltürfunktionen

Im vorigen Wiki-Abschnitt haben wir uns mit der Modulo-Rechnung beschäftigt - diese ist in der Kryptografie wichtig, da einge der Modulo-Rechenarten sind sehr **einfach durchgeführt** werden können, ihre **Umkehrung** oft aber sehr ziemlich **aufwändig** ist.

So kann man die **einfache Rechnung als Verschlüsselung** und die **komplizierte Umkehrung als Entschlüsselung** verwenden – allerding nur dann, wenn es bei der komplizierten Umkehrung eine „versteckte Abkürzung“ gibt, die man als **Schlüssel** nehmen kann.

Eine Funktion, die man einfach berechnen kann, bei der die Umkehrung aber nur mit großem Aufwand berechnet werden kann, nennt man **Einwegfunktion**.

Existiert eine „versteckte Abkürzung“, also eine Zusatzinformation, mit der die ansonsten schwierige Umkehrung einfach gemacht wird, dann spricht man von einer **Falltürfunktion**.