# *Prinzip von Kerkhoff*

Das Prinzip besagt:

**Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.**

Es wäre sehr aufwendig, jeden Tag mathematische Verschlüsselungs-Verfahren zu entwickeln und auf Sicherheit hin zu überprüfen, um sicherzustellen, dass das Verfahren nicht bekannt wird und die Nachricht somit nicht geknackt werden kann.

Aus diesem Grund wird das mathematische Verfahren so gestaltet, dass es von einem weiteren Parameter abhängig ist**: dem Schlüssel**.

Die gleiche Nachricht, mit demselben Verfahren aber mit unterschiedlichen Schlüsseln verschlüsselt, führt zu verschiedenen Chiffren.

Um die Nachricht lesen zu können, muss auf der Empfängerseite nicht nur das Verfahren, sondern auch der Schlüssel bekannt sein – ohne den Schlüssel darf es nicht möglich sein, die Nachricht nur auf Grund der Kenntnis des Verfahrens zu entschlüsseln.

Z.B. verstößt die Caesar-Verschlüsselung gegen diese Vorgabe, denn auch ohne Kenntnis der Verschiebungszahl (=Schlüsse) kann man über die Häufigkeitsanalyse oder noch einfacher durch simples Ausprobieren der 26 möglichen Verschiebungen schnell auf die ursprüngliche Nachricht kommen – einfach nur, weil man das Verfahren kennt.

Das Verfahren ist daher nicht sicher!!!