# Kryptografie

## Caesar-Verschlüsselung

Caesar ist eine der simpelsten Verschlüsselungen und wird heute fast ausschliesslich benutzt, um Kryptografie einfach zu erklären, da es für heutige Verwendungen viel zu unsicher ist.

Geschichte

Laut dem römischen Schriftsteller Gaius Suetonius Tranquillus, wurde die Caesar-Verschlüsselung ursprünglich vom römischen Feldherrn und Diktator Gaius Julius Caesar für militärische Zwecke verwendet. Caesar benutzte hauptsächlich die Verschiebung um 3 Stellen.

### Wie es funktioniert

Für die Verschlüsselung wird zusätzlich zum Klartextalphabet ein Geheimalphabet benutzt, wobei jeder Buchstabe jeweils einem bestimmten verschlüsselten Buchstaben entspricht.

Das verschlüsselte Alphabet erhält man, indem man die Zeichen des lateinischen Alphabets um eine bestimmte Anzahl verschiebt (wobei der Anfang des Klartextalphabets zyklisch am Ende des Alphabets angefügt wird, sodass es aufgeht) und jeweils den Klartextbuchstaben mit dem resultierenden Geheimtextbuchstaben ersetzt.

Beispiel für eine Verschiebung um 10 Buchstaben:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |

Somit wird aus dem Wort «BEISPIEL» «LOSCZSOV», wenn es verschlüsselt wird. Um den Geheimtext wieder zu entschlüsseln wird der ganze Vorgang rückwärts angewandt. Der Schlüssel (der Buchstabe, durch den A ersetzt wird, in diesem Fall

Die Caesar-Verschlüsselung kann auch mathematisch dargestellt werden, indem man jedem der 26 Buchstaben eine Zahl zuordnet (A = 0, B = 1, …, Z = 25). Mit diesen Zahlen kann man die Caesar-Verschlüsselung als ganz einfache Addition darstellen. Dazu wird zum Wert des Klartextbuchstabens **K** einfach der Wert des Schlüsselbuchstabens **S** addiert.

Da es aber Fälle gibt, in denen das Resultat grösser als 25 ist und es keinen Buchstaben mit einem so hohen Wert gibt, muss auf das Resultat eine Modulo-26 Rechnung angewandt werden. Dabei wird der Rest einer Division durch 26 berechnet.

Somit ist die Caesar-Verschlüsselung mathematisch definiert als:

Die dazugehörende Entschlüsselung eines Geheimtextbuchstabens **G** entspricht dann:

### Sicherheit

Da die Caesar-Verschlüsselung eine monoalphabetische Verschlüsselung ist, das heisst, jeder Klartextbuchstabe im Klartextalphabet genau einem Geheimbuchstaben im Geheimalphabet entspricht, kann sie durch Statistik sehr leicht geknackt werden.

Jede Sprache hat eine charakteristische Verteilung der Buchstaben, die leicht in einem Graph aufgezeichnet werden können:

(Graph von der Buchstabenverteilung in der deutschen Sprache einfügen)

Wenn also das ganze Alphabet um beispielsweise 10 Stellen verschoben wird, sieht die Verteilung folgendermassen aus:

(Graph der Buchstabenverteilung 10 Stellen verschoben einfügen)

Da der Verlauf des Graphen immer noch derselbe ist und man weiss, dass E der häufigste Buchstabe ist, kann man nun schliessen, dass das O des Geheimalphabets dem E des Klartextalphabets entspricht. So kann man die Verschiebung berechnen und daraus das Klartextalphabet ableiten.

Da die Buchstabenverteilung jedoch erst in genügend langen Texten genau ist, sollten einzelne Wörter und kurze Sätze in dieser Hinsicht noch einigermassen sicher sein.

Allerdings ist eine weitere Schwäche der Caesar-Verschlüsselung jedoch, dass es nur 25 mögliche Schlüssel gibt, man also spätestens nach 25 Versuchen den Klartext erhält. Vor dieser Angehensweise sind dann auch kurze Sätze und einzelne Wörter nicht mehr sicher.

Im Englischen gibt es zusätzlich noch das Problem, dass es nur zwei Möglichkeiten gibt für Wörter mit einem Buchstaben ("I" = ich und "a" = ein), was das Knacken noch zusätzlich beschleunigt, besonders da beides eher häufige Wörter sind.

### Varianten

Atbasch

Atbasch ist eine ursprünglich auf dem hebräischen Alphabet basierende Variante der Caesar-Verschlüsselung, die auch als umgekehrte Caesar-Verschlüsselung bezeichnet wird, denn statt dass die Buchstaben um eine bestimmte Anzahl Stellen verschoben werden, ist das Geheimalphabet lediglich das Klartextalphabet aber rückwärts, sodass A zu Z wird, B zu Y, und so weiter.

Der Name Atbasch leitet sich dabei von den ersten zwei Buchstabenpaaren ab, die einander ersetzen (Aleph mit Taw und Beth mit Schin)

Speziell an Atbasch ist, dass zum Entschlüsseln der gleiche Prozess benutzt werden kann wie zum Verschlüsseln, da die Buchstaben symmetrisch ausgetauscht werden.

(Beispiel einfügen)

#### ROT13

ROT13 ist eine weitere Variante der Caesar-Verschlüsselung die den gleichen Prozess zum Verschlüsseln und Entschlüsseln benutzt. Hier sind die Buchstaben zwar wie in der normalen Caesar-Verschlüsselung verschoben, aber genau um ein halbes Alphabet, also 13 Stellen. Wenn man also ein Buchstabe verschlüsselt (um 13 Stellen verschiebt) und entschlüsselt (um weitere 13 Stellen verschiebt), hat man den Buchstaben um insgesamt 26 Stellen, also ein ganzes Alphabet verschoben, womit man wieder beim Ausgangsbuchstaben landet.

(Beispiel einfügen)

## Vigenère-Verschlüsselung

### Wie es funktioniert

fdgsdfg

### Geschichte

sdftadfgdfg

### Sicherheit

sdftsdfgdfg

### Varianten

Asdfsdf

#### dasdgsg

sfdgdsfg