1. **Steganografie**

Steganografie ist die Kunst des Versteckens geheimer Nachrichten zum Teil in anderen Nachrichten. Das Ziel ist wie bei der Kryptografie, dass der Geheimtext von niemand unbefugtem gelesen werden kann.

* 1. **Geheimtinte**

Die einfachste Art, einen geheimen Text zu vermitteln, ist natürlich, wenn er gar nicht gesehen werden kann. Dies kann mit verschiedenen Chemikalien erreicht werden, die unter Normalbedingungen farblos sind und entweder durch Hitze, UV-Licht oder chemische Behandlungen sichtbar werden.

* + 1. **Geschichte**

Berichte über Geheimtinte gehen bis weit vor Christus zurück, wo sie im alten Griechenland und im römischen Reich bereits benutzt wurde.

Zumeist wurde Geheimtinte im Krieg benutzt, bevor fortgeschrittene Technologien wie Telegrafen oder Radio entwickelt waren und alle Nachrichten niedergeschrieben und so verschickt werden mussten.

==> <https://www.biodiversitylibrary.org/page/29566341#>

1. **Kryptografie**
   1. **Caesar-Verschlüsselung**

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

* + 1. **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 nach rechts verschiebt und den Klartextbuchstaben mit dem resultierenden Geheimtextbuchstaben ersetzt.

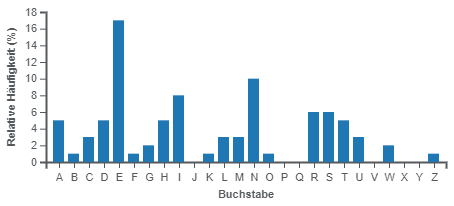
* + 1. **Geschichte**

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.

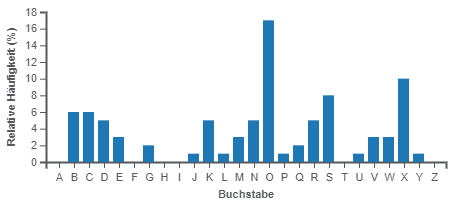
* + 1. **Sicherheit**

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:



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



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.

Eine weitere Schwäche der Caesar-Verschlüsselung ist jedoch, dass es nur 25 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.

* + 1. **Varianten**
       1. **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)

* + - 1. **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)

* 1. **Vigenère**
     1. **Wie es funktioniert**

Anders als bei der Cäsar-Verschlüsselung wird bei der Vigenère-Verschlüsselung ein Schlüssel in Kombination mit 26 Geheimalphabeten benutzt. Dabei wird der Schlüssel so oft wiederholt, bis er die Länge der zu verschlüsselnden Nachricht deckt. …

* + 1. **Geschichte**

1586 präsentierte der Franzose Blaise de Vigenère dem französischen König Henry III eine Art des …

* + 1. **Sicherheit**

…

* + 1. **Varianten**
       1. **Trithemius-Chiffre**

Der Trithemius-Chiffre ist der Vorläufer des Vigenère-Chiffres und wurde vom deutschen Autor und Mönch Johannes Trithemius im frühen 16. Jahrhundert zusammen mit der Tabula Recta erfunden. Für diesen Chiffre benutzt man auch die Tabula Recta aber im Vergleich zu der normalen Vigenère-Chiffre benutzt man keinen Schlüssel, sondern man rückt bei jedem Buchstaben eine Zeile der Tabula Recta weiter nach unten. Im Grunde genommen ist der Trithemius-Chiffre also eine Vigenère-Verschlüsselung mit einem fixen Schlüssel ABCDEFGHIJKLMNOPQRSTUVWXYZ.

* + - 1. **Beaufort Variante**

Da der Vigenère-Chiffre nicht reziprok ist, das heisst dass das Vorgehen des Verschlüsselns nicht das gleiche ist wie das Vorgehen beim Entschlüsseln, kann man auch «in die falsche Richtung» verschlüsseln und den Klartext sozusagen «entschlüsseln», sodass man es nachher mit der normalen Verschlüsselungstechnik wieder entschlüsseln kann. Dies wird als Beaufort Variante bezeichnet und ist nicht zu verwechseln mit dem Beaufort-Chiffre.

* + - 1. **Beaufort-Chiffre**

fg

* + - 1. **Gronsfeld-Chiffre**

fg

* + - 1. **Autokey-Chiffre**

Dies ist die eigentliche Methode, die Blaise de Vigenère erfunden hat

* + - 1. **Running Key Chiffre**

fg

1. Begriffe
   1. Symmetrie <-> Asymmetrie