1. **Geheimtinte**

Die einfachste Art, einen geheimen Text zu vermitteln, ist, wenn er gar nicht erst 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. Diese Art von «Verschlüsselung» gehört nicht zum Themenbereich der Kryptografie, sondern dem der Steganografie. Diese beschäftigt sich mit

dem Verstecken geheimer Nachrichten. Dies geschieht zum Beispiel mit Geheimtinten

oder indem die Nachricht in einer anderen nicht geheimen Nachricht versteckt wird.

Damit ein «leeres» Blatt Papier nicht verdächtig erschien, wurde oft eine unschuldige

Nachricht darauf geschrieben, mit der Geheimnachricht entweder zwischen den Zeilen

oder am Rand des Blattes.

Einer der frühesten Autoren, der unsichtbare Tinte erwähnt, ist Aineias Taktikos, ein

griechischer Stratege und Militärschriftsteller aus dem 4. Jahrhundert v. Chr. Im alten

Griechenland und im römischen Reich wurden Geheimtinten noch zu Kriegszwecken

genutzt, da es damals noch keine elektronische Datenübertragung gab und Nachrichten

zumeist niedergeschrieben wurden, wofür sich Geheimtinte sehr eignete. Später im 17.

bis 19. Jahrhundert erlebten Geheimtinten einen Popularitätsschub, da sie oft benutzt

wurden, um geheime Liebesbriefe zu schreiben.

Die frühesten Formen von unsichtbaren Tinten waren Milch, über die man, wenn sie

angetrocknet war, Kohlestaub oder Asche blasen konnte, der an der getrockneten Milch

kleben blieb und Urin und Fruchtsäfte, deren enthaltene Kohlenhydrate (Kohlenstoff)

bei Erwärmung verkohlen und dunkler werden, wie man es auch zum Beispiel beim

Verbrennen von Holz beobachten kann. Später begann man auch in der Chemie mehr

Möglichkeiten für Geheimtinten zu finden, die zum Teil auch nur auf bestimmte andere

Chemikalien reagierten. Ein Beispiel dafür ist Phenolphthaleinlösung, ein bekannter pH-

Wert Indikator, der bei einem pH-Wert von 0 bis 8,2 farblos ist. Beim Bestreichen mit

einer stärkeren Base wie zum Beispiel einer Ammoniaklösung, wird das Phenolphthalein

pink.

Heutzutage werden Geheimtinten fast ausschliesslich von Kindern für «geheime» Nachrichten genutzt, da sie in der digitalen Welt kaum Anwendung finden und überhaupt nur

sehr schwierig anzuwenden wären, da sie sich fast nur für physisch niedergeschriebene

Nachrichten eignen.

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.

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 Klartextaphabets

zyklisch am Ende des Alphabets angefügt wird, sodass es aufgeht) und jeweils den Klar-

textbuchstaben mit dem resultierenden Geheimtextbuchstaben ersetzt. Um anzugeben

um wie viel das Alphabet verschoben wurde, wird entweder die Anzahl der Stellen der

der Schlüsselbuchstabe (der Buchstabe, durch den A ersetzt wurde) angegeben.

Beispiel für eine Verschiebung um 10 Buchstaben:

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 (in diesem Fall K) wird dabei von A ersetzt.

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 odulo-26 Rechnung

angewandt werden. Dabei wird der Rest einer Division durch 26 berechnet.

Somit ist die Caesar-Verschlüsselung mathematisch definiert als:

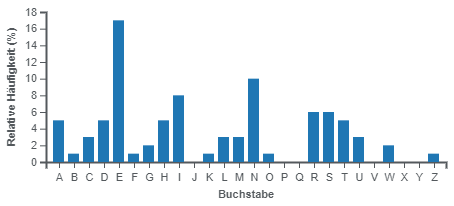
encrypt

Die dazugehörende Entschlüsselung eines Geheimtextbuchstabens G entspricht dann:

decrypt

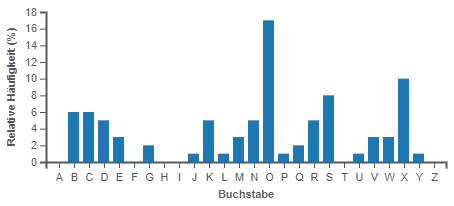
Da die Caesar-Verschlüsselung eine monoalphabetische Verschlüsselung ist, das heisst,

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.

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.

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.

**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.

1. **Vigenère**

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.

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

Da die Vigenère-Verschlüsselung 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 der Beaufort-Verschlüsselung.

Für die Beaufort-Verschlüsselung wird eine ähnliche Tabelle benutzt wie die Tabula Recta, allerdings ist darin das Alphabet auch noch rückwärts. So lautet die erste Zeile ZYXWVUTSRQPONMLKJIHGFEDCBA. Beim Testen dieser Verschlüsselung fiel mir auf, dass sich dabei immer Buchstabentripel bilden, bei denen man immer auf den dritten Buchstaben schliessen kann, wenn zwei bekannt sind und das, egal wie die drei Buchstaben auf Klartext, Geheimtext und Schlüssel verteilt sind. Ein Beispiel dieser Tripel ist AAZ. Wenn also der Klartext ein A ist und der Schlüssel auch, dann wird dieser zu einem Z verschlüsselt. Dank dieser Tripel ist die Beaufort-Verschlüsselung trotz ihrer Sicherheit relativ einfach von Hand zu benutzen, wenn man einmal die Tripel kennt. Da man die Tripel in irgendeiner Reihenfolge lernen kann, können daraus auch gut Eselsbrücken gemacht werden.

Für diese Variante der Vigenère-Verschlüsselung wird ein Schlüssel aus Zahlen benutzt. Da es nur 10 Ziffern gibt, gibt es also auch nur 10 Schlüsselalphabete, was diese Verschlüsselung etwas unsicherer macht als die Vigenère-Verschlüsselung. Was ihre Sicherheit aber verstärkt, ist dass der Schlüssel nicht ein bekanntes Wort sein kann und mit Ziffern mit etwas mehr Unvorhersehbarkeit zu rechnen ist.

Dies ist die eigentliche Methode, die Blaise de Vigenère erfunden hat. Für die Autokey-Verschlüsselung wird ein Schlüssel verwendet, der länger ist als der Klartext. Dafür wird ein Vorschlüssel benutzt, der für die ersten paar Zeichen zum Verschlüsseln benutzt wird. Statt den Schlüssel so lange zu wiederholen, bis er die ganze Länge des Klartexts abdeckt, wird an den Schlüssel der Klartext angehängt. Hat man also einen fünfstelligen Schlüssel, wird für die Verschlüsselung der 6. Stelle des Klartextes, die erste Stelle des Klartextes als Schlüssel benutzt.

Auch bei dieser Variante wird ein Schlüssel benutzt, der mindestens so lang ist wie der Klartext. Hier wird dafür einfach ein langer Schlüssel benutzt. Da diese aber schwieriger sind sich zu merken werden oft Passagen von Büchern oder öffentlichen Texten als Schlüssel benutzt.