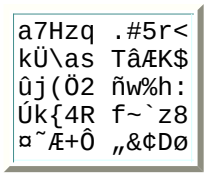
Kryptologie

Verschiebechiffren (CAESAR)



Jeder Buchstabe des Alphabets wird durch einen ersetzt, der eine bestimmte Zahl, *k*, Stellen weiter hinter im Alphabet steht.

Ohne mathematischen Formalismus kann man den Inhalt dieses Abschnitts so zusammenfassen:
Eine Verschiebechiffre wird angewendet, indem jeder Buchstabe eines Textes durch den ersetzt wird, der im Alphabet eine bestimmte Zahl von Stellen weiter hinten steht. Man zählt also einfach, z. B. mit Fingerhilfe: M, M+1 = N, M+2=O, M+3=P, wenn 3 der Schlüssel ist -- also ersetzt man den Buchstaben M durch den Buchstaben P. Kommt man am Ende des Alphabets an, im Beispiel des Standard-Alphabets also bei Z, macht man mit A weiter. Also Y, Y+1=Z, Y+2=A, Y+3=B.
Beim Entschlüsseln geht man umgekehrt vor: Man zählt vom Geheimtext-Buchstaben aus rückwärts.

Beispiele

1.) Original-CAESAR: Hier ist $\Sigma = \{A,...Z\} = Z_{26}$, also A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, ..., Z $\leftrightarrow$ 25. Verwendet wurde von Caesar $k = 3$, also nur ein fester Schlüssel. Die Verschlüsselung sieht dann im Beispiel so aus:

```
C A E S A R  | +3  (Klartext)
-----------
F D H V D U
```

[In Wirklichkeit benutzten die Römer allerdings ein kleineres Alphabet ohne J, U und W.]

Bemerkung. Man kann $K = \mathbf{Z}$ nehmen. Dann ist die Schlüssellänge ∞. Weil aber effektiv nur 26 verschiedene Verschlüsselungsfunktionen erzeugt werden, ist die effektive Schlüssellänge nur $^2\log(26) \approx 4.7$.

2.) ROT13.

3.) XOR.

4.) Dass solch einfache Chiffren auch noch im täglichen Leben verwendet werden, zeigt die abstruse Geschichte des Mafia-Bosses Bernardo Provenzano.

Allgemeine mathematische Beschreibung

Das Alphabet Σ sei eine endliche Gruppe G mit Gruppenoperation *. Als Schlüsselraum wird ebenfalls $K = G$ genommen. Für $k \in K$ sei

$$f_k : \Sigma^* \to \Sigma^*$$

die Fortsetzung der Rechtstranslation $f_k(s) = s*k$ für $s \in \Sigma$, also

$$f_k(a_1,...,a_r) := (a_1*k,...,a_r*k) \quad \text{für} \quad a = (a_1,...,a_r) \in \Sigma^r.$$

Effektive Schlüssellänge: $d(F) = {}^2\log(n)$.

Der Schlüsselraum ist also ziemlich klein und kann leicht vollständig durchsucht werden - Beispiel folgt.

Codes und Chiffren

Eine solche »Vorbehandlung« wie die Zuordnung A ↔ 0 usw., die *nicht geheim* ist, gibt es bei so gut wie allen Verschlüsselungsverfahren; modernes Beispiel ist die Wiedergabe von Dateien durch Bit- oder Bytefolgen. Eine derartige Transformation, die insbesondere nicht von einem Schlüssel abhängt, wird **Codierung** genannt.

> *Was ist eigentlich der Unterschied zwischen »Codierung« und »Chiffrierung«?*

Autor: Klaus Pommerening, 29. September 1999; letzte Änderung: 9. Januar 2008.