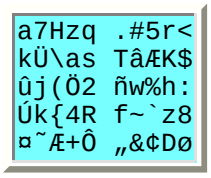
Kryptologie

Verschiebechiffren (CAESAR)



Allgemeine 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

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

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

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

Beispiele

1.) Original-CAESAR: Hier ist Σ = {A,...Z} = $\mathbf{Z}_{26}$ [in Wirklichkeit benutzten die Römer allerdings ein kleineres Alphabet ohne J, U und W], also A ↔ 0, B ↔ 1, ..., Z ↔ 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
```

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.

> Es gibt allerdings auch Chiffrierung mit Hilfe eines Codebuchs, das geheimgehalten wird. Auch für diesen Fall sollte der begrifflichen Klarheit halber nicht die Bezeichnung »Codierung« verwendet werden.

[Der Sprachgebrauch ist, auch in der kryptologischen Literatur, nicht ganz einheitlich; oft werden Chiffren als Codes bezeichnet, manchmal als »geheime Codes«. Im »Alltagssprachgebrauch« (Presse, Literatur) werden die Begriffe »Codierung« und »Chiffrierung«, ebenso »Code« und »Chiffre« bunt durcheinandergemischt.]

Wir merken uns:
Chiffre oder **Verschlüsselung**: Transformation, die von einem geheimen Schlüssel abhängt und daher nur von genau bestimmten Zielpersonen rückgängig gemacht werden kann.
Codierung: Transformation, die nicht geheim ist und daher von jedem rückgängig gemacht werden kann.

2.) ROT13.

3.) XOR.

Autor: Klaus Pommerening, 29. September 1999; letzte Änderung: 12. Oktober 2002.

E-Mail an Pommerening@imsd.uni-mainz.de.