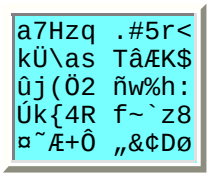
Kryptologie

Lauftext-Chiffrierung



Prinzip

Das Alphabet Σ habe eine Gruppenstruktur mit der Operation *.

Für die Verschlüsselung eines Klartextes $a \in M_r = M \cap \Sigma^r$ verwendet man einen Schlüssel $k \in \Sigma^r$ und bildet

$$\begin{array}{l} a_0\ a_1\ \ldots\ a_{r\text{-}1} \\ k_0\ k_1\ \ldots\ k_{r\text{-}1} \\ \hline c_0\ c_1\ \ldots\ c_{r\text{-}1} \end{array}$$

Verschlüsselt wird also nach der Formel

$$c_i = a_i * k_i \quad \text{für } 0 \le i \le r\text{-}1.$$

Die Entschlüsselungsfunktion ist dann:

$$a_i = c_i * k_i^{-1} \quad \text{für } 0 \le i \le r\text{-}1.$$

Es handelt sich also um eine Verschiebechiffre auf Σ^r.

Von **Lauftext-Chiffre** spricht man, wenn auch der Schlüssel $k \in M_r = M \cap \Sigma^r$, d. h., als sinnvoller Text der Sprache *M* gewählt wird.

Praktischer Hintergrund

Um eine Periode zu vermeiden, muss der Schlüssel einer polyalphabetischen Substitution (mindestens) ebensolang wie der Klartext sein.

Ein Schlüssel soll aber auch leicht zu merken und an den oder die Kommunikationspartner zu verteilen sein.

Daher wurde als Schlüssel oft der Text eines Buches ab einer bestimmten Stelle gewählt (weshalb die Lauttext-Chiffre auch **Buch-Chiffre** genannt wird).

Moderne Version: Inhalt einer CD ab einer bestimmten Stelle.

[Eine andere Möglichkeit, lange Schlüssel zur Verfügung zu haben, besteht darin, algorithmisch aus

einem kurzen Schlüssel einen langen zu erzeugen. Die Beurteilung der Sicherheit dieses Verfahrens ist hochgradig nichttrivial und wird im Kapitel »Bitstrom-Chiffrierung« ausführlich behandelt.]

Beispiel

S = {A,...,Z} = **Z**/*n***Z** als additive Gruppe; die Addition mod 26 erfolgt wie üblich bequem nach der TRITHEMIUS-Tafel (oder »VIGENÈRE-Tableau«).

```
Klartext:   i c h k o m m e m o r g e n u m z e h n
Schlüssel:  V O M E I S E B E F R E I T S I N D S T [ROM UND BAECHE ...]
            ---------------------------------------
Geheimtext: D Q T O W E Q F Q T I K M G M U M H Z G
```

Entschlüsselung durch Subtraktion mod 26, z. B. auch mit Hilfe der TRITHEMIUS-Tafel.

Autor: Klaus Pommerening, 14. Januar 2000; letzte Änderung: 16. Juni 2002

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