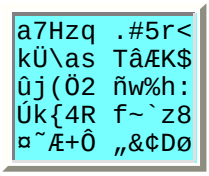
Kryptologie

Mathematisches Modell der Chiffrierung



Kryptographie beschäftigt sich mit der Transformation von Zeichenketten.

Daher wird hier gleich zu Beginn mathematisch formuliert, was damit gemeint ist. Natürlich sind einige (aber nicht viele!) der folgenden Abschnitte auch ohne mathematischen Formalismus verständlich, so dass der Leser ohne mathematische Vorbildung sich hier nicht gleich abschrecken lassen sollte, sondern diesen Abschnitt - und weitere mathematische Abschnitte - einfach überspringen. Es sei aber darauf hingewiesen, dass Kryptologie eine mathematische Wissenschaft ist und man ohne mathematische Formulierungen nicht weit kommt.

Alphabete und Texte

Sei Σ eine endliche Menge; wir nennen sie **Alphabet**.

Beispiele:

- {A, B, ..., Z} = das Standard-Alphabet der klassischen Kryptologie,
- {0, 1} = $\mathbf{F}_2$ = der Körper mit zwei Elementen = Alphabet der Bits,
- $\mathbf{F}_2^8$ = das Alphabet der Bytes (eigentlich: Oktette),
- oder allgemeiner $\mathbf{F}_2^l$ = das Alphabet der l-Bit-Blöcke -
  [oft l = 64, z. B. bei DES oder IDEA oder l = 128, z. B. bei AES].

Das Alphabet Σ wird oft mit einer Gruppenstruktur versehen, z. B.

- Z_n = zyklische Gruppe der Ordnung $n = \#\Sigma$ -
  [Rechnen in dieser Gruppe ist Arithmetik mod n, also elementare Zahlentheorie] -
  Z_n wird als Ring der ganzen Zahlen mod n auch als $\mathbf{Z}/n\mathbf{Z}$ bezeichnet.
- $\mathbf{F}_2$ mit der Körperaddition +, auch als BOOLEsche Operation XOR oder $\oplus$ geschrieben;
- $\mathbf{F}_2^l$ als l-dimensionaler Vektorraum über dem Körper $\mathbf{F}_2$ mit der Vektoraddition, + oder $\oplus$ geschrieben.

Definition

Sei Σ ein Alphabet, Σ^* die Menge aller endlichen Folgen aus Σ; wir nennen solche Folgen »Texte«.

(i) Eine **Verschlüsselungsfunktion** über Σ ist eine injektive Abbildung $f: \Sigma^* \to \Sigma^*$.

(ii) Sei K eine Menge (wir nennen ihre Elemente »Schlüssel«). Eine **Chiffre** (oder Verschlüsselungssystem) über Σ mit Schlüsselraum K ist eine Familie $F = (f_k)_{k \in K}$ von

Verschlüsselungsfunktionen über Σ.

(iii) Sei F eine solche, $F^{\sim} = \{f_k \mid k \in K\} \subseteq \mathrm{Abb}(\Sigma^*,\Sigma^*)$ die zugehörige Menge von (verschiedenen) Verschlüsselungsfunktionen. Dann heißt

$$d(F) := {}^2\log(\#F^{\sim})$$

die **effektive Schlüssellänge** der Chiffre F.

[Beispiele folgen.]

Bemerkungen

1. Die Definition einer Verschlüsselungsfunktion ist nicht die allgemeinste sinnvolle. Man kann auch nicht-injektive Funktionen betrachten, ebenso Relationen, die keine (eindeutigen) Funktionen oder nicht auf ganz Σ^* definiert sind. Die erste und dritte Verallgemeinerung spielen in dieser Vorlesung keine Rolle; die zweite (Nichteindeutigkeit) wird am besten als probabilistische Chiffrierung modelliert.
2. Nicht alle f_k, $k \in K$, müssen verschieden sein; daher ist im allgemeinen $\#F^{\sim} \leq \#K$. Allerdings kann, wenn K unendlich ist, auch $d(F)$ unendlich sein.
3. Oft sind die zu verschlüsselnden Texte nicht allgemeine Zeichenkette, sondern entstammen einer Teilmenge $M \subseteq \Sigma^*$, also einer **Sprache über dem Alphabet** Σ. Man nennt M dann den »Klartextraum« und die Elemente von M »sinnvolle Texte« oder »Klartexte« (englisch: plain texts). Üblicherweise werden allerdings, auch wenn nur Texte aus M verschlüsselt werden sollen, Verschlüsselungsfunktionen auf ganz Σ^* definiert. Die Bildmenge $C_k = f_k(M)$ hängt im allgemeinen vom Schlüssel k ab. Ihre Elemente werden »Geheimtexte« genannt (englisch: cipher texts). Man kann auch den »Geheimtextraum«

   $$C := \cup_{k \in K} C_k$$

   bilden.
4. Durch die Schlüsselwahl wird die Chiffre randomisiert. Auch wenn der Gegner die Verschlüsselungsmethode kennt oder errät, kann er doch ohne den Schlüssel nicht unbefugt entziffern.

Autor: Klaus Pommerening, 25. Oktober 1999; letzte Änderung: 27. April 2002.

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