Kryptologie

Mathematisches Modell der Chiffrierung

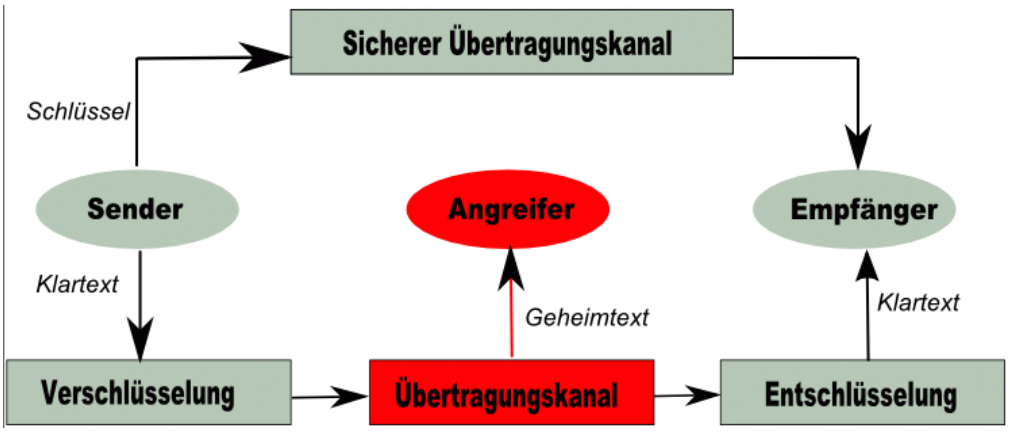
```
a7Hzq .#5r<
kÙ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

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.

Ohne mathematischen Formalismus kann man den Inhalt dieses Abschnitts so zusammenfassen:
Eine Verschlüsselungsfunktion transformiert beliebige Zeichenketten in andere Zeichenketten. (Der Zeichensatz ist dabei vorgegeben.)
Eine Chiffre ist eine parametrisierte Familie von Verschlüsselungsfunktionen. Der Parameter ist der Schlüssel; er bestimmt die Auswahl der konkreten Funktion. Ohne Kenntnis des Schlüssels kann niemand die Verschlüsselung umkehren.

Ziel dieser Transformation ist, dass eine Nachricht (ein Text, eine datei, ...) vor Dritten geheim gehalten werden soll. Diese können zwar sehen, dass da eine Nachricht übermittelt (oder eine Datei gespeichert, ...) wird, können mangels Schlüssel deren Inhalt aber nicht verstehen.



Alphabete und Texte

Sei Σ eine endliche Menge; sie wird in diesem Zusammenhang **Alphabet** genannt und ihre Elemente **Zeichen**.

Beispiele:

- {A, B, ..., Z} = das Standard-Alphabet der klassischen Kryptologie,
- {0, 1} = $\mathbf{F}_2$ = der Körper mit zwei Elementen = Alphabet der Bits - ältester Nachweis bei Bacon 1605 (nach BAUER).
- $\mathbf{F}_2^5$ = das Alphabet des Fernschreibcodes nach BAUDOT (1874) mit 32 verschiedenen Zeichen - dieses Alphabet kommt auch schon bei BACON 1605 vor (nach BAUER).
- $\mathbf{F}_2^8$ = das Alphabet der Bytes (eigentlich: Oktette) - ältester Nachweis bei der IBM um 1964.
- 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 auch als Ring der ganzen Zahlen mod n mit $\mathbf{Z}/n\mathbf{Z}$ bezeichnet.
  Im klassischen Standardbeispiel entspricht das Alphabet {A, B, ..., Z} der Reihe nach den Zahlen {0, 1, ..., 25}.
- $\mathbf{F}_2$ 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.

Sei Σ ein Alphabet, Σ^* die Menge aller endlichen Folgen aus Σ; solche Folgen werden hier **Texte** genannt.

Definition

Gegeben sei ein Alphabet Σ und eine Menge K, die auch unendlich sein kann (ihre Elemente werden hier **Schlüssel** genannt).

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

(ii) Eine **Chiffre** (oder Verschlüsselungssystem oder Kryptosystem) 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

$$^2\log(\#K)$$

die **Schlüssellänge** und

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

die **effektive Schlüssellänge** der Chiffre F.

[Beispiele folgen.]

Bemerkungen

1. Die Definition einer Verschlüsselungsfunktion ist nicht die allgemeinste sinnvolle, siehe dazu das Buch von BAUER. Man kann auch nicht-injektive Funktionen betrachten, ebenso Relationen, die keine (eindeutigen) Funktionen oder nicht auf ganz Σ^* definiert sind. Solche Verallgemeinerungen 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.
   - Die Schlüssellänge der Chiffre ist meist leichter zu bestimmen als die effektive Schlüssellänge, aber praktisch weniger wert.
3. Oft sind die zu verschlüsselnden Texte nicht allgemeine Zeichenketten, 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).
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.

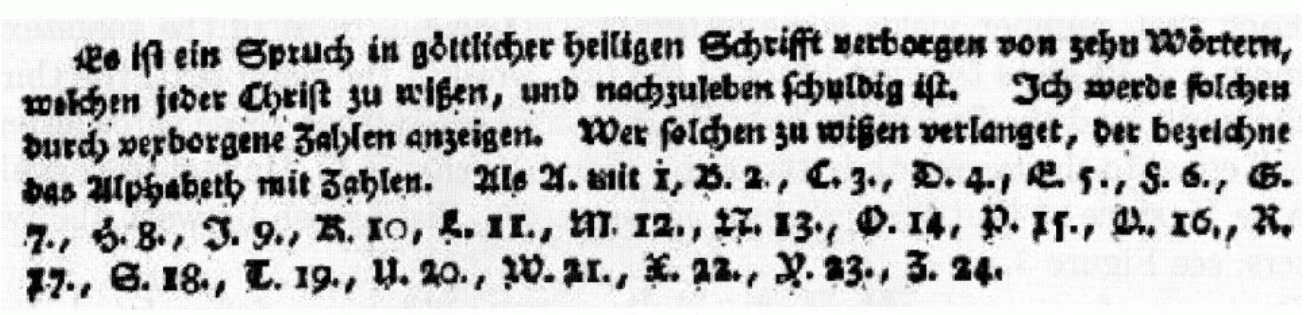
Historisch wurde bei der Zuordnung des gewöhnlichen Alphabets zu Buchstaben meist mit A $\leftrightarrow$ 1 begonnen; solche Zuordnungen gab es schon im Altertum, wo sie zu allerlei Zahlenmystik missbraucht wurden. Zu kryptographischen Zwecken, also um Chiffren arithmetisch zu beschreiben, wurde sie im abendländischen Raum systematisch - soweit bekannt - erstmals von COMIERS verwendet (im Orient allerdings auch schon von Ibn DUNAINIR zu Beginn des 13. Jahrhunderts):

- Claude COMIERS: *L'Art d'Écrire et de Parler Occultement et sans Soupçon*. Paris 1690.

Natürlich ist die Zuordnung A $\leftrightarrow$ 1 statt A $\leftrightarrow$ 0 ungeschickt und führt zu weniger eleganten Formeln. Ein späteres Werk, wo Buchstaben durch Zahlen codiert werden, wurde unlängst von Joachim von zur GATHEN ausgegraben (Friedrich Johann Buck: Arithmetic puzzles in Cryptography. Cryptologia XXVIII (2004), 309 - 324) und online gestellt:

- Friedrich Johann BUCK: *Mathematischer Beweiß: daß die Algebra zur Entdeckung einiger verborgener Schriften bequem angewendet werden könne*. Königsberg 1772.

Aus ihm stammt der Abschnitt


Es iſt ein Spruch in göttlicher heiligen Schrifft verborgen von zehn Wörtern, welchen jeder Chriſt zu wißen, und nachzuleben ſchuldig iſt. Ich werde ſolchen durch verborgene Zahlen anzeigen. Wer ſolchen zu wißen verlanget, der bezeichne das Alphabeth mit Zahlen. Als A. mit 1, B. 2., C. 3., D. 4., E. 5., F. 6., G. 7., H. 8., I. 9., K. 10, L. 11., M. 12., N. 13., O. 14, P. 15., Q. 16., R. 17., S. 18., T. 19., U. 20., W. 21., X. 22., Y. 23., Z. 24.

Autor: Klaus Pommerening, 25. Oktober 1999; letzte Änderung: 9. Dezember 2007.
E-Mail an Pommerening »AT« imbei.uni-mainz.de.