§13. Ausklang

(13.1) Moderne monoalphabetische Verschlüsselungsverfahren

Monoalphabetische Verschlüsselungen von natürlichen Sprachen sind sehr unsicher. Man verwendet deshalb nichtnatürliche Alphabete.

ASCII (American Standard Code for Information Interchange)

Jeder Buchstabe, jede Zahl und jedes Sonderzeichen wird durch eine Folge von 8 Nullen und Einsen dargestellt. So entspricht z.B. dem Buchstaben A die "binäre" Folge

$$\mathbf{0\,1\,0\,0\,0\,0\,0\,1}$$

Jeweils 8 solcher Folgen werden zu einem "Block" zusammengefasst.

Der DES–Algorithmus (Data Encryption Standard)

aus dem Jahre 1977 ist ein monoalphabetisches Verschlüsselungsverfahren über dem Alphabet aller binären Blöcke

$$\{\,(b_1, b_2, b_3, \ldots, b_{64}) \mid b_i \in \{0,1\}\,\}$$

Ein Schlüssel besteht dabei aus 56 binären Zahlen ("Bits"), so dass es insgesamt

$$2^{56} \approx 7 \cdot 10^{16}$$

verschiedene Schlüssel gibt. Trotzdem wurde der DES im Jahre 1999 durch eine vollständige Schlüsselsuche geknackt. Als Verbesserung wurde der

Triple–DES

entwickelt, dessen Schlüssel eine Länge von $\mathbf{112}$ Bits hat.

(13.2) Kryptographie im Alltag

Kryptographische Verfahren sind eigentlich immer im Spiel, wenn sich ein Mensch einem Computer gegenüber ausweisen muss. Beispiele:

- Zugang zu einem Computer mit Hilfe eines Passwortes
- bargeldloser Einkauf mit einer Scheckkarte
- Geldabheben an einem Geldautomaten mit einer Chipkarte
- e–banking
- Handy