Vorlesung vom 16.04.2015

2 Einführung Kryptologie

Kryptologie = Kryptographie + Kryptoanalyse

Kryptographie = kryptos (altgr. geheim) + graphein (altgr. schreiben).

Ursprünglich also Verschlüsselung.
Heute: Design kr. Verfahren für: Verschlüsselung, Authentisierung, ...
Für alle Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit)

Kryptoanalyse = kryptos + analysein (altgr. untersuchen).

Ziel: Ausnutzung von Schwächen oder Beurteilung

Kerckoffsche Prinzipien (niederl. Linguist und Kryptograph,1883):

1. Wenn ein System nicht theoretisch beweisbar sicher ist, so sollte es praktisch sicher sein. (Also mit heutigen Methoden nicht brechbar)
2. Das Design eines System sollte keine Geheimhaltung erfordern (no security by obscurity)

Verschlüsselung

Beispiel. Sei $\Sigma = \{A, B, C, \cdots, Z\} = \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$.

Verschl.: Für Schlüssel $k \in \mathbb{Z}_{26}$: $f_k : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}; x \mapsto (x + k) \mod 26$.

Entschl. Für Schlüssel $k \in \mathbb{Z}_{26}$: $f_k^{-1} : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}; x \mapsto (x - k) \mod 26$.

Verschlüsselung von Texten:

$$F : \Sigma^* \times \mathbb{Z}_{26} \longrightarrow \Sigma^*; ((x_1, \ldots, x_n), k) \mapsto f_k(x_1) \cdots f_k(x_n)$$

Beispiel: $F(\text{CAECAR}, 3) = F(2,0,4,2,0,17, 3) = 5,3,7,5,3,20 = \text{FDHFDU}$.

Nach Kerckoff II: Gegner kennt das Chiffrierverfahren vollständig:

- Zuordnung (oder auch Kodierung) $A \leftrightarrow 0, B \leftrightarrow 1, \ldots$ und
- die Funktion F

Sicherheit hängt von Geheimhaltung des Schlüssels k ab.

Exhaustion des Schlüsselraums: Durchprobieren von 26 Schlüsseln.

Verallgemeinerung:
Beispiel. $\Sigma = \{A, B, C, \cdots, Z\} = \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$.

Ersetze Buchstaben beliebig: A durch D, B durch A, C durch Q, usw.

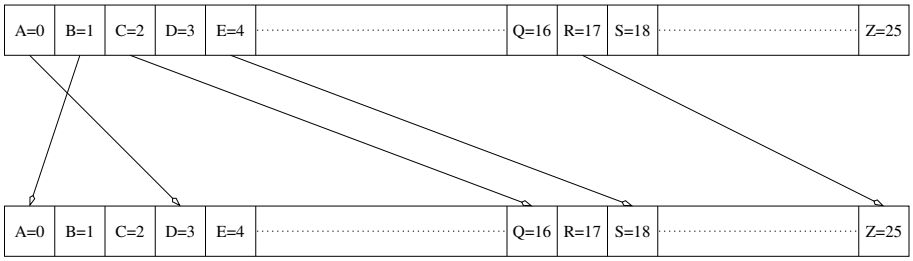

Abbildung 1: Darstellung.

Also $F(\text{CAECAR}) = F((2, 0, 4, 2, 0, 17), k) = \text{QDSQDZ}$.

Anzahl Schlüssel: A kann durch 26 Buchst. ersetzt werden, B durch 25 usw.
$26! \approx 2^{88}$ verschiedene Schlüssel $\Longrightarrow$ Schlüsselexhaustion nicht möglich.

Anderer Angriff: Relative Häufigkeiten von Buchstaben in sinnv. Texten:
E: 17,4%, N: 9,78%, I: 7,55%, ..., Q: 0,02%

Die relativen Häufigkeiten werden übernommen: E $\rightarrow$ S,
S kommt im Chiffretext genauso häufig vor wie E im Klartext.

- Häufigster Buchstabe urspr. E, zweithäufigster urspr. N, usw.
- Rest wird zu sinnvollem Text aufgefüllt.

Solche Angriffen heißen auch statistische Angriffe.

Neue Idee: Ersetze Buchstabenpaare (-tripel). Brechbar mit bekannten Bigramm- bzw. Trigrammhäufigkeiten (ch, ss, tr, en)

Ein absolut sicheres Verschlüsselungsverfahren

Beispiel. (One-Time-Pad)

- Klartexte sind Bitstrings: $(x_1, \ldots, x_n) \in \{0,1\}^n$.
  Z.B. Kodierung über ASCII-Kode $A = 01000001$, $B = 01000010$...
- Schlüssel: $(k_1, \ldots, k_n) \in \{0,1\}^n$.
- Verschl..: $F : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n; (x,k) \mapsto x \oplus k$.
  $\oplus$ ist die komponentenweise Addition modulo 2, d.h.

  $$(x_1, \ldots, x_n) \oplus (k_1, \ldots, k_n) = (x_1 \oplus k_1, \ldots, x_n \oplus k_n)$$

  und $0 \oplus 0 = 0, 1 \oplus 0 = 0 \oplus 1 = 1, 1 \oplus 1 = 0$.
- Entschl..: Wegen $k \oplus k = (0, \ldots, 0)$ gilt $(x \oplus k) \oplus k = x$.

Sicherheit:

Angreifer kennt Chiffretext $y = (y_1, \ldots, y_n) = (x_1 \oplus k_1, \ldots, x_n \oplus k_n)$.

Ziel: Rekonstruktion des Klartextes ohne Kenntnis des Schlüssels.

Schlüssel $k = (k_1, \ldots, k_n)$ zufällig gewählt, d.h. für alle $i \leq n$ gilt

$$\Pr(k_i = 0) = \Pr(k_i = 1) = 1/2 \quad \text{(Münzwurf)}.$$

$$\underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\substack{nicht \\ zufaellig}} \oplus \underbrace{\begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix}}_{zufaellig} = \underbrace{\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}}_{zufaellig} \leftarrow \begin{array}{l} Ist\ Zufallsfolge \\ unabhaengig\ von\ x \end{array}$$

D.h. $\Pr(y_i = 0) = 1/2$ und $\Pr(y_i = 1) = 1/2$ unabhängig von x_i.
y enthält also keinerlei Informationen über den Klartext.

Im informationstheoretischen Sinne: Absolut sicheres Kryptoverfahren gegenüber Angreifer mit unbeschränkten Ressourcen (Rechenkapazität, Zeit)

Nachteil: Schlüssellänge = Textlänge (nicht praktikabel)

Idee: Nutze Schlüssel $k \in \{0,1\}^n$ für mehrere Klartexte $x^1, \ldots, x^m \in \{0,1\}^n$.

- $y^1 \oplus y^2 = (x^1 \oplus k) \oplus (x^2 \oplus k) = x^1 \oplus x^2$.
- $y^2 \oplus y^3 = x^2 \oplus x^3$, $y^1 \oplus y^3 = x^1 \oplus x^3$.

Also: Summe von Klartexten bekannt, ohne Schlüssel zu kennen.

Angriff: (für $n = 128$)

- Ermittle alle sinnvollen Zeichenkombinationen für x^1
  - Länge von x^1 128 Bit, mit ASCII-Kode also genau 16 Zeichen.
  - hh, cc, üü usw. sehr unwahrscheinlich.
- Wähle eine sinnvolle Zeichenkombination aus (Annahme, diese ist der urspr. Klartext)
  - Berechne $x^2 = x^1 \oplus (x^1 \oplus x^2) = x^1 \oplus (y^1 \oplus y^2)$
  - Berechne $x^3 = x^1 \oplus (y^1 \oplus y^3)$
  - Prüfe, ob x^2, x^3 sinnvolle Zeichenkombinationen sind.

Mit steigender Zahl verschlüsselter Klartexte erfolgreich

Frage: Gibt es absolut sichere Verschlüsselungsverfahren ohne den Nachteil des One-Time-Pad (Schlüssel so groß wie der Klartext).

Ergebnis: C.E. Shannon 1948

SAtz 2.1. *Ein Chiffriersystem kann nur dann absolut sicher sein (d.h. gegenüber einem idealisierten Angreifer, der über unbeschränkte Ressourcen verfügt), wenn die eingesetzte Schlüssellänge genauso groß ist wie der zu verschlüsselnde Klartext (genauer Informationsgehalt des Klartextes).*

Kerckoff I: Wenn nicht beweisbar dann praktisch sicher

Wie messen wir Sicherheit?

- Sicherheitsniveau n Bit: Angreifer benötigt zum Brechen 2^n Versuche:
  - Schlüsselexhaustion ($\geq 2^n$ verschiedene Schlüssel)
  - Anderer kryptoanalytischer Methoden (z.B. statistische Angriffe)
- Heute gefordertes Sicherheitsniveau: 128 Bit (d.h. 2^{128} Versuche)
- Sicherheit hängt primär von der Stärke des zugrundeliegenden Alg. ab.
- Aber auch weitere Faktoren sind zu berücksichtigen:
  - Implementierung der Algorithmen
  - Hintergrundsysteme (z.B. für die Zuordnung der Schlüssel zu den Personen, Sicherung eingesetzter Schlüssel)

Was ist 2^{128} für eine Zahl:

- Zeit bis die Sonne zur Nova wird 2^{55} Sekunden
- Alter der Erde 2^{55} Sekunden
- Alter des Universums 2^{59} Sekunden

Annahme: Computer berechnet $2.000.000.000 \approx 2^{31}$ Verschlüsselungen/sec.

Durchprobieren aller 2^{128} möglichen Schlüssel:

$$\frac{\text{Anzahl der möglichen Schlüssel}}{\text{Verschlüsselungen pro Sekunde}} = \frac{2^{128}}{2^{31}} = 2^{97} \text{ Sekunden.}$$