Kryptografie und -analyse, Übung 3

Henry Haustein

Aufgabe 1: Time-Memory-Tradeoff

(a) Wir generieren 2^{25} Schlüssel, für die wir 2^{25} Iterationen berechnen, also haben wir $2^{25} \cdot 2^{25} = 2^{50}$ Schlüssel berechnet. Die Wahrscheinlichkeit ist dann $\frac{2^{50}}{2^{64}} = 2^{-14}$.

(b) Speicheraufwand: # Startschlüssel $\cdot$ Länge(Startschlüssel + Schlüsseltexte) $= 2^{\frac{56}{3}} \cdot 2 \cdot 56$ Bit $= 4.66 \cdot 10^7$ Bit $= 5.83$ MB
Verschlüsselungsoperationen: $2^{\frac{56}{3}} \cdot 2^{\frac{2 \cdot 56}{3}} = 2^{56}$
Der Angreifer findet seinen Schlüssel c_{it} (Aufwand für die Suche: $2^{\frac{56}{3}}$). Damit muss er ausgehend vom Startschlüssel für diese Reihe, k_{i1}, die ganze Reihe neu durchrechnen $\rightarrow 2^{\frac{2 \cdot 56}{3}} - 1$.

Aufgabe 2: Feistel-Chiffre

Aufteilung des Klartextes in 2 Blöcke: $B_1 = 10100110$ und $B_2 = 11001000$, Ver- und Entschlüsselung von Block 1:

- Verschlüsselung:
  - Runde 1, linke Hälfte $L_1 = 0110$, rechte Hälfte $R_1 = S(0110 \oplus 1101) \oplus 1010 = S(1011) \oplus 1010 = 0100 \oplus 1010 = 1110$
  - Runde 2, linke Hälfte $L_2 = 1110$, rechte Hälfte $R_2 = S(1110 \oplus 0001) \oplus 0110 = S(1111) \oplus 0110 = 1011 \oplus 0110 = 1101$

  $\Rightarrow$ Schlüsseltext: 1110|1101
- Entschlüsselung:
  - Runde 1, linke Hälfte $L_1 = S(1110 \oplus 0001) \oplus 1101 = S(1111) \oplus 1101 = 1011 \oplus 1101 = 0110$, rechte Hälfte $R_1 = 1110$,
  - Runde 2, linke Hälfte $L_2 = S(0110 \oplus 1101) \oplus 1110 = S(1011) \oplus 1110 = 0100 \oplus 1110 = 1010$, rechte Hälfte $R_2 = 0110$

  $\Rightarrow$ Klartext: 1010|0110

Aufgabe 3: Designkriterien

Die Abhängigkeitsmatrix ist

	y_3	y_2	y_1	y_0
x_3	0	0	0	1
x_2	0	0	1	0
x_1	1	0	0	0
x_0	0	1	0	0

Die Kriterien sind

- Vollständigkeit: $\forall a_{ij} > 0 \Rightarrow f$ ist nicht vollständig, Grad der Vollständigkeit $\frac{4}{16} = \frac{1}{4}$
- Avalance-Effekt: $\frac{1}{mn} \sum a_{ij} \approx 0.5 \Rightarrow f$ besitzt nicht den Avalance-Effekt
- Linearität: $\forall a_{ij} \in \{0, 1\} \Rightarrow f$ ist linear