



3. Übungsblatt

ÜBUNGEN

G1 (Algebraische Kryptoanalyse).

Gegeben ist folgende Wertetabelle einer einfachen Blockchiffre

Schlüssel k	$E_k(00)$	$E_k(01)$	$E_k(10)$	$E_k(11)$
0	01	00	11	10
1	11	10	01	00

Wir bezeichnen den Schlüssel mit k , den Klartext mit p_1p_2 und den Chiffretext mit c_1c_2 .

Finden Sie zwei Polynome f_1 und $f_2 \in \mathbb{F}_2[k, p_1, p_2]$, so dass für alle Klartexte und alle Schlüssel folgendes gilt: $E_k(p_1p_2) = (f_1(k, p_1, p_2), f_2(k, p_1, p_2))$.

Lösung. Für eine Blockchiffre mit Blocklänge n und m bit langen Schlüssel definieren wir allge mein die Polynome:

$$M_{(X,K)}(p, k) = \left(\prod_{i=1}^n (p_i + X_i + 1) \right) \left(\prod_{j=1}^m (k_j + K_j + 1) \right)$$

Hierbei steht $X = (X_1, \dots, X_n) \in GF(2)^n$ für die Eingabe und $K = (K_1, \dots, K_m) \in GF(2)^m$ für den Schlüssel. In unserem Beispiel erhalten wir so die folgenden Polynome:

$$\begin{aligned} M_{(0,0,0)} &= (p_1 + 1)(p_2 + 1)(k_1 + 1) \\ M_{(0,0,1)} &= (p_1 + 1)(p_2 + 1)(k_1) \\ M_{(0,1,0)} &= (p_1 + 1)(p_2)(k_1 + 1) \\ M_{(0,1,1)} &= (p_1 + 1)(p_2)(k_1) \\ M_{(1,0,0)} &= (p_1)(p_2 + 1)(k_1 + 1) \\ M_{(1,0,1)} &= (p_1)(p_2 + 1)(k_1) \\ M_{(1,1,0)} &= (p_1)(p_2)(k_1 + 1) \\ M_{(1,1,1)} &= (p_1)(p_2)(k_1) \end{aligned}$$

Dabei hat $M_{(X,K)}(p, k)$ nur genau dann den Wert 1, falls $X = p$ und $K = k$. Wir können nun die Verschlüsselungsfunktion wie folgt als Polynom darstellen:

$$P(p, k) = \sum_{X \in GF(2)^n, K \in GF(2)^m} E_K(X) M_{(X,K)}(p, k)$$

Wobei wir $E_K(X)$ als Vektor auffassen. Nun gilt

$$P(p, k) = E_k(p)$$

Für unsere Chiffre erhalten wir so:

$$\begin{aligned}
P(p, k) &= ((p_1 + 1)(p_2 + 1)k + (p_1 + 1)p_2k + p_1(p_2 + 1)(k + 1) + p_1p_2(k + 1), \\
&\quad (p_1 + 1)(p_2 + 1)(k + 1) + (p_1 + 1)(p_2 + 1)k + p_1(p_2 + 1)(k + 1) + p_1(p_2 + 1)k) \\
&= (f_1(p_1, p_2, k), f_2(p_1, p_2, k)) \\
&= E_k(p)
\end{aligned}$$

G2 (Perfekte Sicherheit).

- a) Zeigen Sie, dass das Verschlüsselungsverfahren, das Sie in Aufgabenblatt 1 Aufgabe G3 beschrieben wurde, *perfekt geheim* ist. Gehen Sie davon aus, dass alle Schlüssel mit gleicher Wahrscheinlichkeit gewählt werden.

Lösung. Für jeden Klartext p und jeden Chiffretext c gibt es genau einen einzigen Schlüssel k , so dass p zu c verschlüsselt wird. (k hat den Wert $c - p \pmod{2^n}$) Wir können den Beweis jetzt auf 2 Wegen führen:

- (i) Wir verwenden den Satz von Shannon aus der Vorlesung. Da die Schlüssel alle gleich verteilt gewählt werden, und $\mathcal{P} = \mathcal{C} = \mathcal{K}$ gilt, so ist das Verfahren bereits *perfekt geheim*. (Wir brauchen hier allerdings noch die Nebenbedingung dass $Pr(p) > 0$, für alle Klartexte)
- (ii) Wir zeigen $Pr(p|c) = Pr(p)$. Es gilt $Pr(p|c) = \frac{Pr(c|p)Pr(p)}{Pr(c)}$. Da die Schlüssel gleichverteilt gewählt werden, und so unabhängig vom Klartext jeder Chiffretext mit gleicher Wahrscheinlichkeit gewählt wird (für jeden Schlüssel k entsteht ein anderer Chiffretext), gilt $Pr(c|p) = Pr(c) = 2^{-n} = Pr(c)$. Wir setzen das ein, und erhalten $Pr(p|c) = \frac{2^{-n}Pr(p)}{2^{-n}} = Pr(p)$. Rein formell könnten einige der Wahrscheinlichkeiten nicht definiert sein, da wir hier durch 0 teilen müßten. Wir können aber das Verfahren zu einem äquivalenten Verfahren umdefinieren, wo der Klartextrraum auf die Klartexte eingeschränkt wird, die mit einer Wahrscheinlichkeit von mehr als 0 vorkommen.

- b) Zeigen Sie, dass die lineare Chiffre nicht *perfekt geheim* ist.

Lösung. Angenommen alle Klartexte werden mit gleicher Wahrscheinlichkeit gewählt (jeder Klartext kommt mit Wahrscheinlichkeit 2^{-n} vor). Dann gilt insbesondere $P(p = (0, \dots, 0)) = 2^{-n}$. Bei linearen Chiffren wird dieser Klartext immer auf $(0, \dots, 0)$ abgebildet. Beobachtet ein Angreifer z. B. den Chiffretext $(1, \dots, 1)$, so kann der Klartext nicht $(0, \dots, 0)$ gewesen sein, und es gilt $Pr(p = (0, \dots, 0)|c = (1, \dots, 1)) = 0 \neq Pr(p = (0, \dots, 0)) = 2^{-n}$.

- c) Geben Sie eine Wahrscheinlichkeitsverteilung an, so dass für die lineare Chiffre gilt $Pr(p|c) = Pr(p)$, für alle Klar- und Chiffretexte.

Lösung. Wir wählen einen beliebigen Klartext, z. B. $p_0 = (0, \dots, 0)$, und setzen $Pr(p_0) = 1$. Alle anderen Klartexte kommen mit Wahrscheinlichkeit 0 vor. Nun gilt $Pr(p|c) = Pr(p)$.

G3 (Wahrscheinlichkeitstheorie).

Sei S eine nichtleere Menge, genannt *Ergebnismenge*. Ein *Ereignis* für S ist eine Teilmenge von S . Unter $P(S)$ verstehen wir die *Potenzmenge* von S , also die Menge aller Teilmengen von S . Ein *Ereignis* für S ist ein Element von $P(S)$. A und B schließen sich gegenseitig aus, wenn $A \cap B = \emptyset$ gilt. Eine *Wahrscheinlichkeitsverteilung* auf S ist eine Abbildung $Pr : P(S) \rightarrow \mathbb{R}$ mit den folgenden Eigenschaften:

- a) $Pr(A) \geq 0$ für alle Ereignisse A
b) $Pr(S) = 1$
c) $Pr(A \cup B) = Pr(A) + Pr(B)$, wenn sich A und B gegenseitig ausschließen

Für $A \in P(S)$ heißt $Pr(A)$ die Wahrscheinlichkeit von A . A und B schließen sich gegenseitig aus, wenn $A \cap B = \emptyset$ gilt. A und B heißen unabhängig wenn $Pr(A \cap B) = Pr(A)Pr(B)$ ist. Die Wahrscheinlichkeit A unter der Bedingung B ist $Pr(A|B) = \frac{Pr(A \cap B)}{Pr(B)}$.

Betrachten Sie das Experiment *Würfeln*.

- a) Bestimmen Sie die Ergebnismenge.

$\{1, 2, 3, 4, 5, 6\}$

b) Bestimmen Sie das Ereignis *eine gerade Zahl würfeln*.

$\{2, 4, 6\}$

c) Bestimmen Sie ein davon unabhängiges Ereignis.

Zahl größer 4 würfeln = $\{5, 6\}$

d) Zeigen Sie, dass für $P(A), P(B) > 0$ gilt: $Pr(B)Pr(A|B) = Pr(A)Pr(B|A)$.

$$Pr(B)Pr(A|B) = Pr(B) \frac{Pr(A \cap B)}{Pr(B)} = Pr(A \cap B) = Pr(A) \frac{Pr(B \cap A)}{Pr(A)} = Pr(A)Pr(B|A)$$

e) Bestimmen Sie die Wahrscheinlichkeit dafür, dass eine Zahl < 3 gewürfelt wird, unter der Bedingung, dass das Ergebnis gerade ist.

Wir bezeichnen das Ereignis *Zahl < 3* mit A und das Ereignis *Ergebnis gerade* mit B .

$$Pr(A|B) = \frac{Pr(A \cap B)}{Pr(B)} = \frac{Pr(\{2\})}{Pr(\{2, 4, 6\})} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3}$$