



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: $E_k(p_1p_2) = (f_1(k, p_1, p_2), f_2(k, p_1, p_2))$.

G2 (Perfekte Sicherheit).

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

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:

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

Für $A \in P(S)$ heißt $Pr(A)$ die Wahrscheinlichkeit von A . A und B 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*.

- Bestimmen Sie die Ergebnismenge.
- Bestimmen Sie das Ereignis *eine gerade Zahl würfeln*.
- Bestimmen Sie ein davon unabhängiges Ereignis.
- Zeigen Sie, dass für $P(A), P(B) > 0$ gilt: $Pr(B)Pr(A|B) = Pr(A)Pr(B|A)$.
- Bestimmen Sie die Wahrscheinlichkeit dafür, dass eine Zahl < 3 gewürfelt wird, unter der Bedingung, dass das Ergebnis gerade ist.