



Übungsblatt 6

Aufgabe 1 (Perfekte Sicherheit)

Wir betrachten die affin lineare Blockchiffre über \mathbb{Z}_m mit der Blocklänge 2. Um eine perfekt sicheres Kryptosystem zu erhalten, wird vorgeschlagen, den Schlüsselraum wie folgt einzuschränken:

$$\mathcal{K} = \left\{ (A, B) \in \mathbb{Z}_m^{2 \times 2} \mid A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ und } B = \begin{pmatrix} 0 \\ b \end{pmatrix} \text{ mit } a, b \in \mathbb{Z}_m \right\}.$$

Damit gilt: $|\mathcal{K}| = |\mathcal{C}|$. Für jeden Klartext, der verschlüsselt werden soll, wird ein neuer Schlüssel zufällig und gleichverteilt aus \mathcal{K} gezogen. Kann die Verschlüsselungsfunktion

$$E_{(A,B)} : \mathbb{Z}_m^2 \rightarrow \mathbb{Z}_m^2, x \mapsto Ax + B \pmod{m}$$

perfekt sicher sein? Kann man m so wählen und den Klartextrraum so einschränken, daß die betrachtete Chiffre perfekt sicher wird?

Hinweis: Unterscheiden sie zwischen primen und nicht-primen Moduli m . Nutzen Sie dabei die folgende Version des Satzes von Shannon aus J. Buchmann, „Einführung in die Kryptographie“, 1. Auflage, Berlin Heidelberg New York, Springer 1999:

Satz: Sei $|\mathcal{C}| = |\mathcal{K}|$ und sei die Wahrscheinlichkeit $P(p)$, daß ein bestimmter Klartext $p \in \mathcal{P}$ auftritt größer als 0. Das Kryptosystem ist genau dann perfekt sicher, wenn die Wahrscheinlichkeitsverteilung auf dem Schlüsselraum die Gleichverteilung ist und wenn es für jeden Klartext p und jeden Schlüsseltext c genau einen Schlüssel k gibt mit $E_k(p) = c$.

Aufgabe 2 (Wahrscheinlichkeiten)

Wir betrachten noch einmal die Poker-Variante der 5. Übung. Bei der von uns betrachteten Variante von Poker wird mit einem Blatt von 52 Karten und vier Spielern gespielt. Weiterhin wird das Blatt nach jeder Karte, die ausgeteilt wurde, sofort neu gemischt. Jeder der vier Spieler erhält zu Beginn fünf verdeckte Karten, wobei zuerst der erste Spieler fünf Karten, danach der zweite Spieler fünf Karten usw. erhält. Nach einer Wettrunde hat jeder Spieler die Möglichkeit, bis zu drei Karten auszutauschen.

- (a) Wir betrachten zunächst das folgende einfache Spiel: Es werden vier Karten, nämlich „Pik Dame“ = D_1 , „Herz Dame“ = D_2 , „Pik Bube“ = B_1 und „Herz Bube“ = B_2 gemischt. Dann werden zwei Karten verdeckt vom ersten Spieler gezogen. Spieler zwei zieht daraufhin eine Karte. Spieler Zwei gewinnt, wenn er einen Buben erhält. Wie hoch ist die Wahrscheinlichkeit, daß Spieler zwei gewinnt? Wie hoch ist die Wahrscheinlichkeit, daß Spieler zwei gewinnt, wenn der erste Spieler mindestens eine Dame gezogen hat?
- (b) Nun zurück zum Poker: Sie haben bei den ersten fünf Karten zwei Könige, zwei 7er und einen Buben erhalten. Sie wollen nur den Buben tauschen, und damit ein „Full House“ bekommen. Wir definieren: KD = „Nachbar hat keine Dame“ bzw. KD^c = „Nachbar hat mindestens eine Dame“ und FH = „Full House nach dem Tauschen“. Nehmen wir an, Ihnen sind $P(KD)$ (die Wahrscheinlichkeit, daß das Ereignis KD eintritt), und $P(FH \cap KD)$ (die Wahrscheinlichkeit, daß das Ereignis $KD \cap FH$ eintritt) bekannt. Geben Sie an, wie man mit dieser Kenntnis die Wahrscheinlichkeit von FH unter der Bedingung KD^c berechnen kann.

Hinweis: Benutzen Sie dazu den Satz von Bayes, und die Eigenschaft, daß sich die Wahrscheinlichkeit sich ausschließender Ereignisse summiert.