Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
31. Okt. 2018

Übungen zur Vorlesung Kryptographie
Blatt 3

Aufgabe 9

Man betrachte ein Mini-Kryptosystem mit

$$\mathcal{P} := \{a, b, c\}, \quad \mathcal{C} := \{A, B, C, D\}, \quad \mathcal{K} := \{1, 2, 3, 4\}.$$

Die Verschlüsselung sei durch folgende Tabelle gegeben.

	1	2	3	4
a	C	B	A	C
b	A	C	B	D
c	D	A	D	B

(Das bedeutet z.B. $E_1(a) = C$, $E_3(b) = B$, ...)

Pr_{key} und Pr_{plain} seien jeweils die Gleichverteilung.

a) Man berechne die bedingten Wahrscheinlichkeiten

$$\mathrm{Pr}_{plain|ciph}(x \mid y) \quad \text{für alle } x \in \mathcal{P},\ y \in \mathcal{C}$$

und schließe, dass das Kryptosystem nicht perfekt sicher im Sinne von Shannon ist.

b) Kann man die Verschlüsselungs-Tabelle so abändern, dass bei Gleichverteilung der Schlüssel und beliebiger Verteilung der Klartexte perfekte Sicherheit entsteht?

Aufgabe 10

Für $\nu = 1, 2$ seien $\mathfrak{K}_\nu = (\mathcal{P}_\nu, \mathcal{C}_\nu, \mathcal{K}_\nu, (E_k^{(\nu)}), (D_k^{(\nu)}))$ Kryptosysteme. Daraus kann man ein Produkt-System $\mathfrak{K}_1 \times \mathfrak{K}_2 = (\mathcal{P}, \mathcal{C}, \mathcal{K}, (E_k), (D_k))$ wie folgt definieren:

$$\mathcal{C} := \mathcal{C}_1 \times \mathcal{C}_2, \quad \mathcal{P} := \mathcal{P}_1 \times \mathcal{P}_2, \quad \mathcal{K} := \mathcal{K}_1 \times \mathcal{K}_2$$

und

$$E_{(k_1,k_2)}(x_1, x_2) := (E_{k_1}^{(1)}(x_1), E_{k_2}^{(2)}(x_2))$$

sowie analog für die Entschlüsselungs-Funktion.

Man zeige: Sind $\mathfrak{K}_1$ und $\mathfrak{K}_2$ mit gegebenen Wahrscheinlichkeits-Verteilungen auf den Klartext- und Schlüssel-Räumen perfekt sicher im Sinne von Shannon, so ist auch das Produkt-System mit den (unabhangigen) Produkt-Verteilungen perfekt sicher.

Aufgabe 11

Wir betrachten folgendes Kryptosystem: Sei $N = 2n$ eine positive gerade Zahl. Klartext- und Geheimtext-Menge seien definiert durch $\mathcal{P} := \mathcal{C} := \mathbb{Z}_2^N$. Als Schlüsselmenge $\mathcal{K}$ diene die Gruppe S_N aller Permutationen der Menge $\{1, 2, \ldots, N\}$. Dabei ist für $\pi \in \mathcal{K}$ die Verschlüsselung $E_\pi : \mathcal{P} \to \mathcal{C}$ durch Permutation der Komponenten eines Klartext-Vektors $x \in \mathbb{Z}_2^N$ gemäß π gegeben. Für die Entschlüsselung $D_\pi : \mathcal{C} \to \mathcal{P}$ gilt daher $D_\pi = E_{\pi^{-1}}$. Wir wählen als Pr_{key} die Gleichverteilung auf $\mathcal{K}$. Weiter sei Pr_{plain} eine beliebige Wahrscheinlichkeits-Verteilung auf $\mathcal{P}$ mit $\mathrm{Pr}_{plain}(x) > 0$ für alle $x \in \mathcal{P}$.

Man zeige: Das beschriebene Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, (E_\pi), (D_\pi))$ bietet keine perfekte Sicherheit im Sinne von Shannon.

Aufgabe 12 (Fortsetzung von Aufgabe 11)

Man betrachte das folgende Teilsystem des in der vorigen Aufgabe betrachteten Kryptosystems: Sei $\mathcal{P}_1 = \mathcal{C}_1$ die Menge aller Vektoren $x = (x_1, \ldots, x_N) \in \mathbb{Z}_2^N$, so dass genau n der Komponenten x_i verschwinden.

a) Aus wievielen Elementen besteht $\mathcal{P}_1$? Man zeige, dass für jede Permutation $\pi \in \mathcal{K} = S_N$ gilt $E_\pi(\mathcal{P}_1) = \mathcal{C}_1$, dass also $\mathcal{K}$ auch als Schlüsselraum für das Teilsystem benutzt werden kann.

b) Man beweise, dass das Teilsystem $(\mathcal{P}_1, \mathcal{C}_1, \mathcal{K}, (E_\pi), (D_\pi))$ mit den vom Gesamtsystem induzierten Wahrscheinlichkeits-Verteilungen perfekte Sicherheit im Sinne von Shannon liefert.
