

2. Übungsblatt
Kryptographie I (SS 2006)

Stefan Lucks, Emin Islam Tatli

Besprechung: Mittwoch, 10. Mai 2006

Aufgabe 1

- a) Die PIN-Nummer einer heutigen EC-Karte besteht aus 4 Dezimalziffern. Jede der Ziffern wird gleichverteilt und unabhängig von den anderen aus der Menge $\{0, \dots, 9\}$ gezogen. Wie groß ist die Entropie einer solchen PIN-Nummer?
- b) Bis vor einigen Jahren wurden PIN-Nummern von EC-Karten aus 4 gleichverteilten und unabhängigen Hexadezimalziffern $h_i \in \{0, \dots, F\}$ abgeleitet. Die i -te Stelle s_i der PIN-Nummer wurde aus der i -ten Hexadezimalziffer h_i berechnet nach der Regel

$$s_i = h_i \bmod 10.$$

Wie groß war die Entropie dieser alten PIN-Nummern?

- c) Beschreibe für die Schlüssel aus a) und b) jeweils einen möglichst effizienten Algorithmus zur Schlüsselsuche. Wie viele Schlüssel müssen jeweils im Mittel getestet werden, um den richtigen zu finden?

Aufgabe 2 Seien die Buchstaben a, \dots, z , die Ziffern $0, \dots, 9$ und das Leerzeichen in den Zahlen $\{0, \dots, 36\} = \mathbb{Z}_{37}$ codiert. Für ein Tupel $(a, b) \in \mathcal{K} \subseteq \mathbb{Z}_{37} \times \mathbb{Z}_{37}$ sei folgende Abbildung definiert:

$$f_{a,b}(x) := a \cdot x + b \pmod{37}, \quad x \in \mathbb{Z}_{37}$$

Für welche der angegebenen Verschlüsselungsfunktionen $E_{a,b}$ zusammen mit der jeweiligen Schlüsselmenge \mathcal{K} und Klartextmenge \mathcal{P} kann man eine Chiffretextmenge \mathcal{C} und eine Entschlüsselungsfunktion $D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{P}$ angeben, so dass $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D)$ eine Chiffre ist? Welche der Chiffren sind perfekt? Es wird dabei angenommen, dass jeder Schlüssel mit gleicher Wahrscheinlichkeit auftritt, analog für jeden Klartext.

- a) $E_{a,b}(x) := f_{a,b}(x)$, $\mathcal{K} = \mathbb{Z}_{37}^\times \times \mathbb{Z}_{37}$, $\mathcal{P} = \mathbb{Z}_{37}$, wobei $\mathbb{Z}_{37}^\times = \{1, \dots, 36\}$ ist.
- b) $E_{a,b}((x, x')) := (f_{a,b}(x), f_{a,b}(x'))$, $\mathcal{K} = \mathbb{Z}_{37}^\times \times \mathbb{Z}_{37}$, $\mathcal{P} = \mathbb{Z}_{37} \times \mathbb{Z}_{37}$

- c) $E_{a,b}((x, x')) := (f_{a,b}(x), f_{a,b}(x')), \mathcal{K} = \mathbb{Z}_{37}^\times \times \mathbb{Z}_{37}, \mathcal{P} = \{(x, x') \in \mathbb{Z}_{37} \times \mathbb{Z}_{37} \mid x \neq x'\}$
- d) $E_{a,b}(x) := f_{a,b}(x), \mathcal{K} = \mathbb{Z}_{37}^\times \times \mathbb{Z}_{37}^\times, \mathcal{P} = \mathbb{Z}_{37}$
- e) $E_{a,b}(x) := f_{a,b}(x), \mathcal{K} = \mathbb{Z}_{37} \times \mathbb{Z}_{37}, \mathcal{P} = \mathbb{Z}_{37}$

Aufgabe 3 Sei Q eine Quelle von n Elementen, q_1, \dots, q_n , die mit der Wahrscheinlichkeit p_i auftreten. Die Shannon-Entropie H und die Min-Entropie H_{\min} sind definiert durch

$$H(Q) := - \sum_{i=1}^n p_i \cdot \log_2(p_i)$$

$$H_{\min}(Q) := -\log_2(p) \text{ mit } p := \max\{p_1, \dots, p_n\}$$

Zeige dass gilt:

- a) $0 \leq H_{\min}(Q) \leq H(Q)$
- b) Q ist gleichverteilt $\iff H_{\min}(Q) = H(Q)$

Berechne $H_{\min}(Q)$ für die Quellen aus Aufgabe 1, a) + b) und für eine Quelle, die alle 26 Buchstaben gemäß der auf dem letzten Übungsblatt gegebenen Verteilung produziert.

Aufgabe 4 Zeige, dass für zwei Zahlen $a, b \in \mathbb{Z}$ gilt:

- a) $(a + b) \bmod n = (a \bmod n) + (b \bmod n) \bmod n$
- b) $(a \cdot b) \bmod n = (a \bmod n) \cdot (b \bmod n) \bmod n$