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

WS 2011/12
30. Nov. 2011

Einführung in die Kryptographie

Übungsblatt 4

Aufgabe 13

Es sei $\sigma : \mathfrak{A} \to \mathfrak{A}$ eine zufällige Permutation des Alphabets $\mathfrak{A} = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \cong \mathbb{Z}_{26}$, wobei jede Permutation gleich wahrscheinlich sei. Man berechne die Wahrscheinlichkeit dafür, dass σ (mindestens) einen Fixpunkt besitzt, d.h. ein $x \in \mathfrak{A}$ existiert mit $\sigma(x) = x$.

Aufgabe 14

Sei $N = 2n$ eine positive gerade Zahl und $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^N$. Sei $\mathcal{K} = S_N$ die Gruppe aller Permutationen der Menge $\{1, 2, \ldots, N\}$. Für $\pi \in \mathcal{K}$ sei $E_\pi : \mathcal{P} \to \mathcal{C}$ die Verschlüsselung, die durch Permutation der Komponenten eines Klartext-Vektors $x \in \mathbb{Z}_2^N$ gemäß π entsteht. Sei $\mathbb{P}_{key}$ die Gleichverteilung auf $\mathcal{K}$ und $\mathbb{P}_{plain}$ eine beliebige Wahrscheinlichkeits-Verteilung auf $\mathcal{P}$ mit $\mathbb{P}_{plain}(x) > 0$ für alle $x \in \mathcal{P}$.

a) Man zeige: Das Chiffriersystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, \mathbb{P}_{plain}, \mathbb{P}_{key})$ bietet keine perfekte Sicherheit im Sinne von Shannon.

b) Man betrachte das folgende Teilsystem: 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. Man zeige: Das Chiffriersystem $(\mathcal{P}_1, \mathcal{C}_1, \mathcal{K}, E, \mathbb{P}_{plain1}, \mathbb{P}_{key})$ liefert perfekte Sicherheit. Dabei ist $\mathbb{P}_{plain1}$ eine beliebige Wahrscheinlichkeits-Verteilung auf $\mathcal{P}_1$ mit $\mathbb{P}_{plain1}(x) > 0$ für alle $x \in \mathcal{P}_1$.

Aufgabe 15

Die Folge $z_i \in \mathbb{Z}_{25}$, $i \geqslant 0$, wurde durch einen 'linearen Kongruenz-Generator'

$$f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}, \quad z \mapsto (az + b) \bmod 25,$$

mit einem Anfangselement $z_0 \in \mathbb{Z}_{25}$ durch die Rekursionsformel $z_{i+1} = f(z_i)$ erzeugt. Wir identifizieren $\mathbb{Z}_{25}$ mit dem Alphabet `A`, ..., `Z`, wobei `I/J` als ein Buchstabe gelte.

Der folgende Geheimtext entstand aus einem englischen Klartext durch Addition der Folge (z_i) modulo 25.

```
LHHBLADYTXIUCZDDKPKVTLZXNEG
```

Der Klartext beginnt mit dem Trigramm `THE`. Man berechne a, b und bestimme den Klartext.

---

b.w.

Aufgabe 16

Es sei

$$N := 345\,30400\,34910\,50447\,62362\,62840\,08424\,37869\,41885\,28545\,79337\,35797$$

der Modul eines Blum-Blum-Shub Pseudo-Zufallsgenerators, d.h. $N = pq$ mit Primzahlen $p \equiv q \equiv 3 \bmod 4$. Ausgehend von einem quadratischen Rest $z_0 \in (\mathbb{Z}/N)^*$ sei die Folge $(z_i)_{i \geqslant 0}$ rekursiv definiert durch $z_{i+1} := z_i^2 \bmod N$. Diese Folge definiert eine Folge von Bits durch $b_i := z_i \bmod 2$.

Der folgende Geheimtext der Länge von 64 Bytes

```
41F0 D6C8 8434 EB27 AF37 A024 C1B0 8BA7 8D4B 502C 5E67 5792
1D74 2C7B 4BC2 4A02 1FBF 0C13 3894 C000 2DDB ED09 11C6 F0E5
D92D D1D9 0D92 715D 6756 62FD A1E0 208A
```

entstand aus einem Klartext von 39 Bytes auf folgende Weise: Die Bits $(b_i)_{0 \leqslant i < 312}$ wurden zu einem One-Time-Pad der Länge 39 Bytes (= 312 Bits) zusammengefasst. (Jeweils 8 Bits $\beta_0, \beta_1, \ldots, \beta_7$ ergeben ein Byte $\xi = \sum_{i=0}^{7} \beta_i \cdot 2^i$.) Das One-Time-Pad wurde mit der Operation XOR auf den Klartext addiert, was die ersten 39 Bytes des Geheimtextes liefert. Anschließend folgt ein Nullbyte und dann 24 Bytes, welche die Zahl z_{312} in hexadezimaler Schreibweise darstellen.

a) Man entschlüssele den Geheimtext.

b)* Man bestimme die Periode der Folge (z_i).