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

WS 2015/16
4. Nov. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 3

Aufgabe 9

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 10

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. Die Folge $(z_1, z_2, \ldots, z_N) \in \mathbb{Z}_{25}^N$ werde als Pseudo-One-Time-Pad aufgefasst. Wir identifizieren $\mathbb{Z}_{25}$ mit dem Alphabet `A`, ..., `Z`, wobei `I/J` als ein Buchstabe gelte.

Der folgende Geheimtext der Länge $N = 27$ entstand aus einem englischen Klartext durch Addition modulo 25 des oben beschriebenen Pseudo-One-Time-Pads.

```
LHHBLADYTXIUCZDDKPKVTLZXNEG
```

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

---

b.w.

Aufgabe 11

a) Sei $F(X) = \sum_{\nu=0}^{n} a_\nu X^\nu \in \mathbb{F}_2[X]$, $a_n = 1$, ein irreduzibles Polynom vom Grad $n > 1$ über dem Körper $\mathbb{F}_2$. Man zeige:

(i) $a_0 = 1$.

(ii) Die Anzahl der $\nu \in \{0, 1, \ldots, n\}$ mit $a_\nu = 1$ ist ungerade.

(iii) Das "gespiegelte" Polynom

$$G(X) = \sum_{\nu=0}^{n} a_\nu X^{n-\nu}$$

ist ebenfalls irreduzibel.

b) Man erstelle eine Liste aller irreduziblen Polynome über $\mathbb{F}_2$ vom Grad $\leqslant 5$.

Aufgabe 12

Die Elemente des Körpers $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(\varphi(X))$, wobei φ das irreduzible Polynom

$$\varphi(X) = X^4 + X + 1 \in \mathbb{F}_2[X]$$

bezeichnet, seien mit 4-Bit-Zahlen identifiziert, wobei $\xi = \sum_{i=0}^{3} a_i 2^i$ dem Körperelement $\sum a_i X^i \bmod \varphi(X)$ entspreche. Wir benutzen hexadezimale Notation für die 4-Bit-Zahlen.

a) Sei $u :=$ `'2'`, $v :=$ `'A'`. Man berechne $u + v$, $u \cdot v$, u^3 und u^5.

b) Man beweise: Das Element $u =$ `'2'` ist eine Primitivwurzel von $\mathbb{F}_{2^4}^*$, d.h. ein erzeugendes Element der multiplikativen Gruppe $\mathbb{F}_{2^4}^*$.