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

WS 2015/16
28. Okt. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 2

Aufgabe 5 Sei $m \geqslant 2$ und

$$\mathcal{P} := \{\vec{p} = (p_i)_{i\in\mathbb{Z}_m} \in \mathbb{R}^m : \sum_{i\in\mathbb{Z}_m} p_i = 1 \text{ und } p_i \geqslant 0 \text{ für alle } i \in \mathbb{Z}_m\}$$

die Menge aller Wahrscheinlichkeits-Verteilungen auf $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. Für $\vec{p}, \vec{q} \in \mathcal{P}$ ist das *Faltungs-Produkt* $\vec{r} = \vec{p} * \vec{q} \in \mathcal{P}$ definiert durch

$$r_k := \sum_{i\in\mathbb{Z}_m} p_i q_{k-i}.$$

a) Man zeige, dass $\vec{p} * \vec{q}$ wieder zu $\mathcal{P}$ gehört und dass das Faltungs-Produkt kommutativ und assoziativ ist, d.h.

$$\vec{p} * \vec{q} = \vec{q} * \vec{p} \quad \text{and} \quad (\vec{p} * \vec{q}) * \vec{r} = \vec{p} * (\vec{q} * \vec{r}) \quad \text{für alle } \vec{p}, \vec{q}, \vec{r} \in \mathcal{P}.$$

b) Seien

$$x = (x_1, \ldots, x_N) \in \mathbb{Z}_m^N \quad \text{und} \quad y = (y_1, \ldots, y_N) \in \mathbb{Z}_m^N$$

Zufallstexte über dem Alphabet $\mathbb{Z}_m$, wobei die Zeichen x_ν unabhängig voneinander gemäß der Wahrscheinlichkeits-Verteilung $\vec{p} = (p_i)_{i\in\mathbb{Z}_m}$ und die Zeichen y_ν unabhängig voneinander gemäß der Wahrscheinlichkeits-Verteilung $\vec{q} = (q_i)_{i\in\mathbb{Z}_m}$ gewählt wurden.
Man zeige: Ist $z := x + y \in \mathbb{Z}_m^N$ der Text, der daraus durch Addition modulo m entsteht, so haben die Zeichen von z die Wahrscheinlichkeits-Verteilung $\vec{p} * \vec{q}$.

Aufgabe 6

Sei $\mathcal{P}$ wie in Aufgabe 5 und $\vec{u} = (u_i) \in \mathcal{P}$ die Gleichverteilung, d.h. $u_i = 1/m$ für alle $i \in \mathbb{Z}_m$.

a) Man zeige, dass die Funktion

$$F : \mathcal{P} \longrightarrow \mathbb{R}, \quad F(\vec{p}) := \sum_{i\in\mathbb{Z}_m} p_i^2$$

genau im Punkt $\vec{u} \in \mathcal{P}$ ihr absolutes Minimum annimmt.

b) Man zeige, dass

$$\vec{u} * \vec{p} = \vec{p} * \vec{u} = \vec{u} \quad \text{für alle } \vec{p} \in \mathcal{P}.$$

c) Sei $\vec{p} = (p_i) \in \mathcal{P}$ eine Verteilung mit $p_i > 0$ für alle $i \in \mathbb{Z}_m$. Man beweise: Die Folge

$$\vec{p}^{\,n} := \underbrace{\vec{p} * \ldots * \vec{p}}_{n\text{-mal}}, \qquad n = 1, 2, 3, \ldots$$

konvergiert für $n \to \infty$ gegen die Gleichverteilung $\vec{u} \in \mathcal{P}$.

Aufgabe 7

Sei $n \geqslant 2$ und σ eine Permutation der Menge $\{1, 2, \ldots, n\}$. Eine *Transpositions-Chiffre* $T = T_{n,\sigma}$ werde wie folgt definiert: Der Klartext wird in Blöcke von n^2 Zeichen unterteilt. Diese Zeichen werden als die n Zeilen $(x_{i1}, x_{i2}, \ldots, x_{in})$, $i = 1, 2, \ldots, n$, einer $n \times n$-Matrix geschrieben. Der transformierte Block ist die Folge der Spalten $(x_{1\sigma(j)}, x_{2\sigma(j)}, \ldots, x_{n\sigma(j)})$, $j = 1, 2, \ldots, n$, in der permutierten Reihenfolge. (Falls der letzte Block aus weniger als n^2 Zeichen besteht, wird nur der obere Teil der Matrix gefüllt, und die Spalten werden kürzer.)

Der folgende Geheimtext entstand aus einem deutschen Klartext der Länge 36 mit dem oben beschriebenen Verfahren für $n = 6$.

`IURUEMESEASKFSDOIRRTSMETERZRVATKUEDN`

a) Man finde den Klartext und die Permutation σ.

b) Man bestimme die kleinste ganze Zahl $N \geqslant 1$, so dass $T_{6,\sigma}^N = \mathrm{id}$.

Aufgabe 8 (CBC-Modus monoalphabetischer Verschlüsselungen)

Sei $\mathfrak{A} = \{A, B, \ldots, Z\} \cong \mathbb{Z}_{26}$ und $\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ eine Permutation. Der CBC-Modus der monoalphabetischen Verschlüsselung, die durch σ gegeben wird, ist wie folgt definiert: Sei

$$x = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}_{26}^N$$

der Klartext und $y_0 \in \mathbb{Z}_{26}$ ein beliebig vorgegebenes Element. Dann ist der verschlüsselte Text $y = (y_1, \ldots, y_N)$ definiert durch

$$y_i := \sigma(x_i + y_{i-1}) \quad \text{für } i = 1, \ldots, N.$$

Hier bezeichnet + die Addition modulo 26.

(*Bemerkung.* Die Buchstaben CBC stehen für *cipher block chaining*.)

a) Man verschlüssele den Text `AAAAAAAAAAAAAAAAAAAAAAAAA` im CBC-Modus zum Caesar-Shift

$$\sigma = \sigma_d : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto x + d,$$

mit $d = 5, 6, 13$ und $y_0 = 3$.

b) Man zeige: Ist $\sigma = \sigma_d$ ein Caesar-Shift, so lässt sich die Entschlüsselung des CBC-Modus zu σ_d auf die Entschlüsselung eines gewöhnlichen Caesar-Shifts zurückführen.

c) Man entschlüssele den Geheimtext

`NWIREVTPYISBTQXJOXWCSBMRXTGPFKBYDURPUF`

der mit dem CBC-Modus eines Caesar-Shifts erzeugt worden ist.