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

WS 2011/12
16. Nov. 2011

Einführung in die Kryptographie

Übungsblatt 3

Aufgabe 9*

Der folgende Geheimtext entstand aus einem deutschen Klartext im CBC-Modus zu einer monoalphabetischen Substitution $\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, vgl. Aufgabe 4.

```
UMSET ZIOOL JNFNH GELDA BYWIL GLUOZ DTULQ OFJPL WDTAS AXHAC ZLQIZ IXGOP
LLFNY KVWTV FSASN JJRXS NJWCE HBZZK WCUTK SJCLR PPLWP NHACW SMLSY SEVXE
WNHMU WGQZT PRNUW NHAJG ERJPO KVPUD RWOKI HJGEA FNSAM XYZTV RPZLG CRSWY
AMXYZ IPTPR JYIYU TUBGD JHKCU AYNUW NNPLA MFBSR OZIDT EOZQM YEOTV BNYWN
QQTCS XIBFL VTVOP GXQOT AFUWU MXEVW RNQMS BQJCL HKSRN QWDXV XFNMM HWHAZ
IXKKF HARQT BQGYL GVUDT EOZXJ ZJCLF NXYKF RREOK DUDTG YDMGE TVBVI YHACM
FBZSA SNMHG WWIBF QZEOP NJMJZ AOTBQ ZWHWT TVCRS WQMXZ JZCUQ MKEJD TUFKC
IBKSR WOTVO IXAZE OYHBB QWFVI FSBRP UGMVU SUUUT VOMBP TAIHX CRXGF WSUTV
CDMMQ VTVFC SKFQJ ZZUTZ KIAJC EAMXY DMQIB PDVOJ OESQG FA
```

Man entschlüssele den Text und bestimme σ.

Hinweis. Man betrachte Bigramme x_0y des Geheimtextes mit festem x_0 und variablem y.

Aufgabe 10

Seien $x = (x_1, \ldots, x_N) \in \mathbb{Z}_m^N$ und $y = (y_1, \ldots, y_N) \in \mathbb{Z}_m^N$ Zufallstexte über dem Alphabet $\mathbb{Z}_m$, wobei die Zeichen x_n unabhängig voneinander gemäß der Wahrscheinlichkeits-Verteilung $\vec{p} = (p_i)_{i\in\mathbb{Z}_m}$ und die Zeichen y_n gemäß der Wahrscheinlichkeits-Verteilung $\vec{q} = (q_i)_{i\in\mathbb{Z}_m}$ gewählt werden.

a) Man berechne den Erwartungswert $\mathbb{E}\,\kappa(x, y)$ des Kappa-Index von x and y.

b) Sei speziell $q_i = p_{\sigma(i)}$ für eine Permutation $\sigma : \mathbb{Z}_m \to \mathbb{Z}_m$. Man beweise, dass für festes $\vec{p}$ und variables σ das absolute Maximum von $\mathbb{E}\,\kappa(x, y)$ für $\sigma = \mathrm{id}_{\mathbb{Z}_m}$ angenommen wird.

Aufgabe 11

Sei

$$\mathcal{P} := \{\vec{p} = (p_i)_{i\in\mathbb{Z}_m} \in \mathbb{R}^m : \sum_{i\in\mathbb{Z}_m} p_i = 1 \text{ and } p_i \geq 0 \text{ for all } i \in \mathbb{Z}_m\}$$

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

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

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

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

b) Seien $x, y \in \mathbb{Z}_m^N$ Texte wie in Aufgabe 10, und $z := x+y \in \mathbb{Z}_m^N$ der Text, der daraus durch Addition modulo m entsteht. Man zeige, dass die Zeichen von z die Wahrscheinlichkeits-Verteilung $\vec{p} * \vec{q}$ haben.

Aufgabe 12

Sei $\mathcal{P}$ wie in Aufgabe 11 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

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

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

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

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

Anleitung. Sei M_n das Maximum der Komponenten von $\vec{p}^{\,n}$. Man zeige, dass die Folge $(M_n)_{n\in\mathbb{N}}$ monoton fällt.
