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

WS 2018/19
24. Okt. 2018

Übungen zur Vorlesung Kryptographie

Blatt 2

Aufgabe 5

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 $n = 6$.

`NLIFAIEEERKGELNDHGNTUMASUUGOLOEHNMLH`

Man finde den Klartext und die Permutation σ.

Aufgabe 6 (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.

a) Man verschlüssele den Text `AAAAAAAAAAAAAAAAAAAAAAAAAA` (der Länge 26) im CBC-Modus zum Caesar-Shift

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

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

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

c) Man entschlüssele den Geheimtext

`SINAXGOXXKVEWFBKAJPNWJAXGNZDMYQOXPDIUQCBTBKGE`

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

---

b.w.

Aufgabe 7

Es sei $\mathrm{GL}(2,\mathbb{Z}_{26}) = \{A \in M(2\times 2,\mathbb{Z}_{26}) : \gcd(\det(A),26) = 1\}$ die Menge aller invertierbaren 2×2-Matrizen mit Koeffizienten aus $\mathbb{Z}_{26}$ und $\mathrm{Aff}(2,\mathbb{Z}_{26})$ die Menge aller Abbildungen

$$\psi : Z_{26}^2 \to \mathbb{Z}_{26}^2, \quad x \mapsto \psi(x) := Ax + t, \quad A \in \mathrm{GL}(2,\mathbb{Z}_{26}),\ t \in \mathbb{Z}_{26}^2.$$

a) Man zeige, dass $\mathrm{Aff}(2,\mathbb{Z}_{26})$ bzgl. der Komposition von Abbildungen eine Gruppe bildet. Aus wievielen Elementen besteht diese Gruppe?

b) Vermöge der Identifikation $\{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z}\} \mathrel{\widehat{=}} \mathbb{Z}_{26}$ kann man die Elemente aus $\mathrm{Aff}(2,\mathbb{Z}_{26})$ als Bigramm-Substitutionen auffassen. Man bestimme, falls möglich, Transformationen aus $\mathrm{Aff}(2,\mathbb{Z}_{26})$, die `ALBERT` in `JOSEPH` bzw. in `JOHANN` überführen.

Aufgabe 8

Sei $\mathfrak{A} = \{A_1, A_2, \ldots, A_m\}$ ein aus m Zeichen bestehendes Alphabet und seien

$$X = (x_1, x_2, \ldots, x_N) \in \mathfrak{A}^N, \quad Y = (y_1, y_2, \ldots, y_N) \in \mathfrak{A}^N$$

zwei Texte der Länge N über dem Alphabet $\mathfrak{A}$. Der *Koinzidenz-Index* von X und Y ist definiert als

$$\kappa(X,Y) := \frac{1}{N}\sum_{\nu=1}^{N} \delta(x_\nu, y_\nu), \quad \text{wobei} \quad \delta(x,y) := \begin{cases} 1, & \text{falls } x = y, \\ 0, & \text{falls } x \neq y. \end{cases}$$

Es sei weiter eine Wahrscheinlichkeits-Verteilung auf $\mathfrak{A}$ gegeben, bzgl. der das Zeichen A_i die Wahrscheinlichkeit p_i, $0 \leqslant p_i \leqslant 1$, besitzt, wobei $\sum_{i=1}^m p_i = 1$.

a) Man zeige: Wählt man in den Texten X, Y die Zeichen x_ν, y_ν unabhängig voneinander mit den gegebenen Wahrscheinlichkeiten, so gilt für den Erwartungswert des Koinzidenz-Index die Formel $\quad \mathbb{E}\left[\kappa(X,Y)\right] = \sum_{i=1}^{m} p_i^2.$

b) Es sei $\varrho : \mathfrak{A}^N \to \mathfrak{A}^N$ die zyklische Rotation um 1 nach links, d.h.

$$\varrho(x_1, x_2, \ldots, x_N) := (x_2, x_3, \ldots, x_N, x_1);$$

also ϱ^k die zylische Rotation um k Stellen nach links.
Der Φ-Index eines Textes $X \in \mathfrak{A}^N$, $(N \geqslant 2)$, ist definiert als

$$\Phi(X) := \frac{1}{N-1}\sum_{k=1}^{N-1} \kappa(X, \varrho^k(X)).$$

Man zeige:

$$\Phi(X) = \frac{1}{N(N-1)}\sum_{i=1}^{m} f_i(f_i - 1).$$

Dabei bezeichnet f_i die Anzahl des Vorkommens von A_i im Text X.

c) (Invarianz-Eigenschaft) Ist $\sigma : \mathfrak{A} \to \mathfrak{A}$ eine bijektive Abbildung und $\sigma(X)$ der aus X durch die monoalphabetische Substitution σ entstandene Text, so gilt

$$\Phi(X) = \Phi(\sigma(X)).$$