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

WS 2011/12
2. Nov. 2011

Einführung in die Kryptographie

Übungsblatt 2

Aufgabe 5

Man zeige: Eine Abbildung der Gestalt

$$\varphi_{ab} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad x \mapsto ax + b, \quad a \text{ invertierbar in } \mathbb{Z}_{26},$$

mit $\varphi_{ab} \neq \mathrm{id}$ ist entweder fixpunktfrei oder hat genau 2 Fixpunkte.

Aufgabe 6

Es sei $G := \mathrm{GL}(2, \mathbb{Z}_{26})$ die Gruppe aller invertierbaren 2×2-Matrizen über dem Ring $\mathbb{Z}_{26}$. Man bestimme die Anzahl der Elemente von G.

Aufgabe 7

Es bezeichne $\mathrm{Aff}(2, \mathbb{Z}_{26})$ 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.

b) Vermöge der Identifikation $\{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\} \cong \mathbb{Z}_{26}$ 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 $n \geqslant 2$ 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 25 mit dem oben beschriebenen Verfahren für $n = 5$.

`NZEOM EIRRU EFNLT FEAIS IITGH`

a) Man finde den Klartext und die Permutation σ.

b) Man bestimme die kleinste ganze Zahl $N \geqslant 1$, so dass $T_{5,\sigma}^N = \mathrm{id}$.