Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 23.10.2015

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 1

AUFGABE 1:

a) Geben Sie ein Beispiel für ein Kryptosystem an, dessen Verschlüsselungsfunktionen zwar injektiv aber nicht surjektiv sind.

b) Betrachten Sie ein Kryptosystem mit $|\mathcal{P}| = m$ und $|\mathcal{C}| = n$, wobei $m < n$. Wie viele verschiedene Verschlüsselungsfunktionen kann dieses Kryptosystem höchstens besitzen?

AUFGABE 2:

Wir betrachten die Permutations-Chiffre wie in der Vorlesung definiert mit $\mathcal{P} = \mathcal{C} = \Sigma^n$, $\Sigma = \{A, B, \ldots, Z\}$ und $n = 6$.

a) In der Vorlesung haben wir gesehen, wie Elemente des Schlüsselraums $\mathcal{K}$ als Liste von Urbildern und Bildern dargestellt werden können. Welches der folgenden, in dieser Weise dargestellten Elemente ist in $\mathcal{K}$ enthalten?

$$\begin{pmatrix} A & B & C & D & E & F \\ C & D & E & B & F & A \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 5 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 1 & 2 & 7 \end{pmatrix}$$

b) Verschlüsseln Sie die Nachricht „KRYPTO“ mit den gültigen Schlüsseln aus a).

c) Wie lautet jeweils der zugehörige Schlüssel für die Entschlüsselungsfunktion?

AUFGABE 3:

Gegeben sei die Matrix

$$A = \begin{pmatrix} 9 & 10 & 2 \\ 1 & 13 & 5 \\ 6 & 8 & 3 \end{pmatrix} \in \mathbb{Z}_{15}^{3\times 3}.$$

a) Besitzt A ein Inverses in $\mathbb{Z}_{15}^{3\times 3}$?

b) Berechnen Sie gegebenenfalls das Inverse mit der Cramerschen Regel aus der Vorlesung.