Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 23.10.2015 **Abgabe:** Mo. 2.11.2015 bis 14:45 Uhr

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 1

AUFGABE 1 (10 Punkte)**:**
Wir betrachten die folgende *affin-lineare* Verallgemeinerung der Caesar-Chiffre: Zu $\alpha, \beta \in \mathbb{Z}$ wird ein Buchstabe x mit Hilfe der Vorschrift

$$x \mapsto (\alpha x + \beta) \bmod 26$$

verschlüsselt. Dabei identifizieren wir die Buchstabenmenge $\{A, B, \ldots, Z\}$ mit den Elementen des Ringes $\mathbb{Z}_{26}$. Die Verschlüsselung einer langen Nachricht entsteht dadurch, dass Zeichen für Zeichen die Verschlüsselung der Buchstaben hintereinander geschrieben wird.

a) Seien $\alpha = 11$ und $\beta = 4$. Entschlüsseln Sie den Geheimtext "SQF".

b) Geben Sie eine formale Definition der affin-linearen Caesar-Chiffre als 5-Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ an.

c) Welche Eigenschaften müssen gelten, damit alle Nachrichten eindeutig entschlüsselbar sind? Achten Sie darauf bei Ihrer Definition!

d) Wie viele unterschiedliche Verschlüsselungsfunktionen gibt es?

AUFGABE 2 (8 Punkte)**:**

a) Wir betrachten das *Hill-Kryptosystem* mit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^3$ und dem geheimen Schlüssel

$$A = \begin{pmatrix} 25 & 21 & 13 \\ 25 & 8 & 16 \\ 11 & 8 & 21 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3}.$$

Entschlüsseln Sie den Chiffretext $c = \begin{pmatrix} 11 \\ 16 \\ 5 \end{pmatrix} \in \mathbb{Z}_{26}^3$.

b) Ein Schlüssel $k \in \mathcal{K}$ eines Kryptosystems heißt *selbst-invers*, wenn für alle $m \in \mathcal{P}$ gilt $E_k(E_k(m)) = m$. Konstruieren Sie für eine Hill-Chiffre mit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{15}^4$ einen selbst-inversen Schlüssel $A \in \mathcal{K}$, für den $\det(A) \not\equiv \pm 1 \pmod{15}$ gilt.

AUFGABE 3 (6 Punkte)**:**
Wir betrachten die Permutations-Chiffre wie in der Vorlesung definiert mit $\mathcal{P} = \mathcal{C} = \Sigma^n$, $|\Sigma| = m$, mit $m, n \in \mathbb{N}$.

a) Wie groß ist der Schlüsselraum $\mathcal{K}$?

b) Seien $\pi_1, \pi_2 \in \mathcal{K}$ zwei Schlüssel. Zeigen Sie, dass für $E_{\pi_1}, E_{\pi_2} \in \mathcal{E}$ gilt:

$$E_{\pi_2} \circ E_{\pi_1} = E_{\pi_1 \circ \pi_2}.$$

Hier sei $\circ$ der Operator für die Verkettung von Funktionen.

c) Sie fangen den Schlüsseltext $c = 21110151$ für den Fall $\Sigma = \{x \in \mathbb{N}_0 : x < 10\}$, $n = 8$ ab, der das Datum des nächsten geplanten Überfalls auf die Paderborner Sparkasse im Format YYYY:MM:DD veschlüsselt. Wann ist mit einem Überfall zu rechnen?