TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

1. Übung Kryptographie

1. Aufgabe

Sei Σ ein endliches Alphabet und $\mathcal{P} = \Sigma^n = \mathcal{C}$, d.h. die Menge der Klartexte ist gleich der Menge der Verschlüsselungstexte und bezeichne $\mathcal{K}$ den Schlüsselraum. Wir betrachten ein symmetrisches Verschlüsselungsverfahren, welches die folgenden beiden Bedingungen erfüllt:

(a)
$$\forall k \in \mathcal{K}\, \forall M \in \mathcal{P} :\ \mathcal{D}(k, \mathcal{E}(k, M)) = M,$$

(b)
$$\forall k_1, k_2 \in \mathcal{K} \text{ mit } k_1 \neq k_2\ \exists M \in \mathcal{P} :\ \mathcal{E}(k_1, M) \neq \mathcal{E}(k_2, M).$$

Beweist, dass
$$|\mathcal{K}| \leq (|\Sigma^n|)!$$
gilt.

(4 Punkte)

2. Aufgabe

(a) Sei $(G, \circ)$ eine endliche Gruppe. Ein Verschlüsselungssystem benutzt $\mathcal{P} = G$ als Klartextraum und es gelte $\mathcal{P} = \mathcal{C} = \mathcal{K}$. Als Verschlüsselungsfunktion wird
$$\mathcal{E} : \mathcal{K} \times \mathcal{P} \longrightarrow \mathcal{C}, \quad k \circ m = c$$
benutzt. Unter welchen Voraussetzungen und Annahmen ist dieses System perfekt sicher? Warum?

(b) Gibt es Bedingungen unter denen der Vigenère-Chiffre perfekt sicher ist?

(4 Punkte)

3. Aufgabe

(a) Seien $\Sigma = \{0, \ldots, 25\}$, $n \in \mathbb{N}$ und $\mathcal{P} = \Sigma^n$ und definiere
$$\mathcal{E} : \mathcal{P} \times \Sigma \to \Sigma^n\ ,\ (a_1, \ldots, a_n, k) \mapsto (ka_1 \mod 26, \ldots, ka_n \mod 26)$$
Auf welche Teilmenge $\mathcal{P} \times \mathcal{K} \subseteq \mathcal{P} \times \Sigma$ eingeschränkt liefert $\mathcal{E}$ eine Verschlüsslungsfunktion? Wie sieht der Chiffretextraum aus? Gebt eine Entschlüsslungsfunktion an.

(b) Als Verallgemeinerung davon betrachte $\Sigma = \{0, 1\}$, $n \in \mathbb{N}$ und $\mathcal{P} = \Sigma^n$ mit

$$\mathcal{E} : \mathcal{P} \times \Sigma^{n \times n} \to \Sigma^n \ , \ (a_1, \ldots, a_n, A) \mapsto (a_1, \ldots, a_n)A.$$

Verschlüsselt wird also durch Multiplikation mit einer Matrix über $\mathbb{Z}/2\mathbb{Z}$. Auf welche Teilmenge $\mathcal{K} \subseteq \Sigma^{n \times n}$ eingeschränkt liefert $\mathcal{E}$ eine Verschlüsslungsfunktion? Gebt eine Entschlüsslungsfunktion an. Wie könnte ein Known Plaintext Angriff gegen dieses System aussehen?

(6 Punkte)

4. Aufgabe

Implementieren Sie die Verschlüsselungs- und Entschlüsselungsfunktion des Vigenère Kryptoverfahrens mit gegebener Schlüssellänge $n \in \mathbb{N}$ und dem Alphabet $\Sigma = \{A, \ldots, Z\}$.

(6 Punkte)