1. Übung Kryptographie

1. Aufgabe

- (a) Sei Σ ein endliches Alphabet und Σ^* die Menge aller Worte bezüglich Σ . Ferner bezeichne ε das leere Wort von Σ^* . Nun sei durch

$$\sigma : (\Sigma^*, \Sigma^*) \longrightarrow \Sigma^*, \quad ((w_{11}, \dots, w_{1n}), (w_{21}, \dots, w_{2m})) \longmapsto ((w_{11}, \dots, w_{1n}, w_{21}, \dots, w_{2m}))$$

eine binäre Verknüpfung auf Σ^* gegeben ($m, n \in \mathbb{N}$). Zeigen Sie, daß Σ^* bezüglich σ ein Monoid ist.

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

(i)

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

(ii)

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

Beweisen Sie, daß

$$|\mathcal{K}| \leq (|\Sigma^n|)!$$

gilt.

(4 Punkte)

2. Aufgabe

Zeigen Sie, dass ein bezüglich IND-CCA2 sicheres Verschlüsselungsverfahren notwendigerweise probabilistisch sein muss.

(3 Punkte)

3. Aufgabe

Sei ϕ in der Übung erwähnte Euler ϕ -Funktion. Ferner sei $n \in \mathbb{N}$ mit Primfaktorzerlegung

$$n = \prod_{i=1}^t p_i^{k_i},$$

wobei p_i verschiedene Primzahlen und $k_i > 0$ sind. Zeigen Sie die folgende Gleichheit:

$$\phi(n) = \prod_{i=1}^t (p_i^{k_i} - p_i^{k_i-1})$$

(4 Punkte)

4. Aufgabe

Seien $\Sigma = \{0, \dots, 25\}$, $n \in \mathbb{N}$ und $\mathcal{P} = \Sigma^n$ und definiere

$$\mathcal{E} : \mathcal{P} \times \Sigma \rightarrow \Sigma^n, (a_1, \dots, a_n, k) \mapsto (ka_1 \bmod 26, \dots, ka_n \bmod 26)$$

Auf welche Teilmenge $\mathcal{P} \times \mathcal{K} \subseteq \mathcal{P} \times \Sigma$ eingeschränkt liefert $\mathcal{E}$ eine Verschlüsselungsfunktion? Wie sieht der Schlüsseltextrraum aus? Geben sie eine Entschlüsselungsfunktion an.

(3 Punkte)

5. Aufgabe

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

(6 Punkte)