1. Übung Kryptographie

(Grundlagen, Affin-lineare Blockchiffren, Angriffsmodelle)

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

Ein Klartext M wurde mit einem Vigenère Blockchiffre zu dem Chiffretext C verschlüsselt mit dem Alphabet $\Sigma = \{A, \dots, Z\}$. Bestimmen Sie den Schlüssel und den Klartext M . Bestimmen Sie dazu die Schlüssellänge mittels einiger Perioden und benutzen Sie folgende Statistik.

C=UQHTXQVFILUIQFYDWGKKMRBMVMTUOINISGWEXFOGTHVKODCCZSSVNVLUIAOGTXZOX
 PIEBIDWPNPQMRXYZKRORQVXUQYYAOOMXVURAHRXHQIKVNIEMIZZBTMZJBXQMXVURQRV
 TEZHRXIZHNZIZHVKWUGUKVTIVZHQVFZISEAUKDECNMQFRXYTXQGMYSJEEWRORPVVZXQV
 VNVQZRXAQRQARSRVILFFRSIDOGUHQVJKRZIEJEHSACIUWFKVPIAARHIEYGTPHKWEIYZIZ
 MANEXXAOGTXRXOQRAKRWEAT

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6.51	n	9.78
b	1.89	o	2.51
c	3.06	p	0.79
d	5.08	q	0.02
e	17.40	r	7.00
f	1.66	s	7.27
g	3.01	t	6.15
h	4.76	u	4.35
i	7.55	v	0.67
j	0.27	w	1.89
k	1.21	x	0.03
l	3.44	y	0.04
m	2.53	z	1.13

Tabelle 1: Relative Buchstabenhäufigkeiten in der deutschen Sprache in Prozent

(5 Punkte)

4. 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)

5. Aufgabe

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

(5 Punkte)