TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

1. Übung Kryptographie

1. Aufgabe **Permutationen endlicher Alphabete** **(4 Punkte)**

(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

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

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.

2. Aufgabe **Affin-linearer Blockchiffre** **(4 Punkte)**

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

C = EKFUFTAVFZUBEKFPUBJONGSBTGITAIVVAWNB WAAFKHGOBXKFBMGJEIVAFFTACGH-JPANJPFCSGAEIKGHSGAAVBCTFEIGOBJUUC

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

3. Aufgabe **Elementare Wahrscheinlichkeitstheorie** **(4 Punkte)**

Sei A das Ereignis, daß man im ersten Wurf eines 6-seitigen "idealen" Würfels eine 2 würfelt und B das Ereignis daß man beim zweiten Wurf eine 6 würfelt.

(a) Geben Sie einen geeigneten Wahrscheinlichkeitsraum an.

(b) Beschreiben Sie A und B als Teilmengen des Wahrscheinlichkeitsraumes.

(c) Was ist $Pr(A \cup B)$?

(d) Zeigen Sie, daß A und B unabhängig sind.

Sei nun X die Zufallsvariable, die die Punkte eines Würfelwurf angibt.

(a) Was ist der Erwartungswert $E(X)$ von X?

(b) Was ist der Erwartungswert für die Summe der Punktanzahlen, die man bei zwei Würfelwürfen erhält? Was ist der Erwartungswert für das Produkt der Punktanzahlen?

(c) Was ist die erwartete Anzahl von Zweier-Würfen, damit die Summe der Punktanzahlen größer gleich 8 ist? Finden Sie eine untere Schranke für die Anzahl der Zweier-Würfe, damit die Summe der Punktanzahlen mit Wahrscheinlichkeit 2/3 größer gleich 8 ist.

4. Aufgabe **Praktische Aufgabe** **(8 Punkte)**

(a) Sei $g \in \mathbb{N}$ und $g > 1$. Schreibe in KASH3 ein Programm, welches die g-adische Entwicklung eines Elementes $a \in \mathbb{N}$ berechnet.

(b) Schreibe in KASH3 ein Programm, welches für zwei Polynome $g, f \in \mathbb{Q}[x]$ Elemente $u, v \in \mathbb{Q}[x]$ berechnet mit $ug + vf = \mathrm{ggT}(f, g)$.

Wichtige Befehle: Floor, Log, PolynomialAlgebra, mod