TECHNISCHE UNIVERSITÄT BERLIN Sommersemester 2004
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto`

5. Übung Kryptographie

1. Aufgabe Ordnung von Gruppenelementen (4 Punkte)

(i) Sei G eine endliche Gruppe und $|G| = \prod_{i=1}^{n} p_i^{e_i}$ die Zerlegung der Gruppenordnung in seine Primfaktoren. Sei $g \in G$ beliebig aber fest. Für jeden Primteiler p_i von G bezeichne der Ausdruck $f(p_i)$ die größte ganze Zahl mit $g^{|G|/p_i^{f(p_i)}} = 1$. Zeigen Sie, daß

$$Ord(g) = \prod_{i=1}^{n} p_i^{e_i - f(p_i)}$$

gilt für $g \in G$, wobei $Ord(g)$ die kleinste Zahl $n \in \mathbb{N}$ ist mit $g^n = 1$.

(ii) Sei $g \in G$ ein Element einer endlichen Gruppe G. Um seine Ordnung $m \in \mathbb{N}$ zu ermitteln wählen wir zufällig k ganze Zahlen e_i $(1 \leq i \leq k)$ und berechnen $a_i = g^{e_i}$. Sobald zwei Exponenten e_i und e_j gefunden sind mit $g^{e_i} = g^{e_j}$ ist $g^{e_i - e_j} = 1$, d.h. $e_i - e_j = m \cdot l =: \alpha$ mit $l \in \mathbb{N}$. Indem man α faktorisiert, kann man mit (i) die Ordnung von g finden. Wie groß muß k sein, damit die Wahrscheinlichkeit dafür, daß ein solches Vielfaches gefunden wird, größer als $\frac{1}{2}$ ist?

2. Aufgabe Chinesischer Restsatz (4 Punkte)

(a) Sei $n = pq$ mit $p, q > 2$ verschiedene Primzahlen und $a, b \in \mathbb{N}$ mit $ab \equiv 1 \mod (p-1)(q-1)$. Zeigen Sie, daß für beliebiges $x \in \mathbb{Z}/n\mathbb{Z}$ gilt: $x^{ba} \equiv x \mod n$.

(b) Sei $m \in \mathbb{N}$ und $m \geq 2$ mit Primfaktorzerlegung $m = \prod_{i=1}^{n} p_i^{n_i}$ gegeben. Zeigen Sie, daß für die eulersche ϕ-Funktion

$$\phi(m) = \prod_{i=1}^{n} (p_i - 1) \cdot p_i^{n_i - 1}$$

gilt.

3. Aufgabe Praktische Aufgabe (12 Punkte)

Folgendes Verfahren wird benutzt um Nachrichten zu verschlüsseln: Gegeben sei $n = 965137$ und $b = 23049$. Wir betrachten das Alphabet

$$\{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\},$$

wobei A die Position 0 hat, B die Position 1 usw. Worte werden wie folgt verschlüsselt:

Ist ein Wort gegeben, z.B. "HALLO", so wird zuerst eine Liste L der Positionen der Buchstaben des gegeben Wortes im Alphabet erstellt. Hier wäre das $[7, 0, 11, 11, 14]$, d.h. also $H \leftrightarrow 7$, $A \leftrightarrow 0$ usw. Dann wird daraus eine Zahl $k \in \mathbb{N}$ berechnet wie folgt:

$$k = 7 \cdot 26^4 + 0 \cdot 26^3 + 11 \cdot 26^2 + 11 \cdot 26 + 14,$$

also eine 26-adische Darstellung. Schließlich berechnet man $k^b \mod n$. Gegeben ist nun eine Liste M von Zahlen, die eine verschlüsselte Nachricht darstellen:

```
M =  [ 235418, 310753, 841777, 213399, 944992, 287096, 291512,
 240666,  14167, 883847, 897646, 338123, 837633, 788315, 196474,
52661, 128826, 709512,281367, 334413, 344646, 770181, 468276,
341011 ].
```

Entschlüsseln Sie die Nachricht mit Hilfe eines KASH-Programmes. Benutzen Sie dabei die Funktionen **IntXGcd** (der erweiterte euklidische Algorithmus) und **Factor** (zum Faktorisieren von ganzen Zahlen).

Gesamt: 20 Punkte