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

7. Übung Kryptographie

1. Aufgabe Cycling-Attacke (4 Punkte)

Sei (n, e) ein öffentlicher RSA-Schlüssel. Für einen Klartext $m \in \{0, 1, ..., n-1\}$ sei $c \equiv m^e \mod n$ der zugehörige Schlüsseltext. Zeigen Sie, daß es eine natürliche Zahl k gibt mit

$$m^{e^k} \equiv m \mod n.$$

Beweisen Sie für ein solches k:

$$c^{e^{k-1}} \equiv m \mod n.$$

Ist dies eine Bedrohung für RSA? Begründen Sie ihre Antwort.

2. Aufgabe Jacobi-Symbol (2 Punkte)

Berechne folgende Ausrücke und schreibe dabei jeden einzelnen Rechenschritt auf:

(i) $\left(\frac{4628}{6409}\right)$

(ii) $\left(\frac{873475982374598}{8085}\right)$

3. Aufgabe Franklin-Reiter (6 Punkte)

Sei $R := (\mathbb{Z}/n\mathbb{Z})[x]$. Die restlichen Bezeichnungen sind hier wie im Skript gewählt. Im Franklin-Reiter Related Message Angriff gilt für $e = 3$ und $f(x) = ax + b \in R$ mit $a, b \neq 0 \mod n$, dass sich entweder der RSA-Modul n faktorisieren läßt oder aber $\deg(\mathrm{ggT}(g, h)) = 1$ ist.

(a) Kann der euklidische Algorithmus in R immer funktionieren?

(b) Gib ein Gegenbeispiel an wo der euklidische Algorithmus in R fehlschlägt.

(c) Zeige: Wenn der euklidische Algorithmus scheitert, so haben wir n faktorisiert.

4. Aufgabe **Praktische Aufgabe** **(8 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 **XGCD** (der erweiterte euklidische Algorithmus) und **Factorisation** (zum Faktorisieren von ganzen Zahlen).