TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
www.math.tu-berlin.de/∼hess/krypto-ws2007

Abgabe: 07.12.2007
in der Übung

7. Übung Kryptographie

(RSA Kryptosystem und Sicherheitsaspekte)

---

1. Aufgabe

Seien $(n_A, 3), (n_B, 3), (n_C, 3)$ und $(n_A, 7)$ RSA öffentliche Schlüssel von Alice, Bob, Calvin beziehungsweise Dana, die in einem öffentlichen Netzwerk miteinander kommunizieren. Franck verschlüsselt eine Nachricht m mit den öffentichen Schlüsseln und schickt an Alice, Bob, Calvin und Dana zu. Erklären Sie, wie Eve die ursprüngliche Nachricht m bestimmen kann, falls sie die folgenden Informationen erhällt:

- Verschlüsselung der Nachricht m gesendet an Alice, Bob und Calvin.
- Verschlüsselung der Nachricht m gesendet an Alice und Dana.
- Die Zahlen e und d mit $a^{ed} \equiv a \mod n_A$ fr alle $a \in \mathbb{Z}$ mit gcd$(a, n_A) = 1$.
- Den Wert von $\phi(n_B)$, wobei ϕ Eulersche $\phi-$ Funktion ist.

(5 Punkte)

2. Aufgabe

(a) Sei $n = p \cdot q$, wobei p und q verschiedene ungerade Primzahlen sind. Ferner sei $a \cdot b \equiv 1 \mod \lambda(n)$, wobei $a, b \in \mathbb{Z}$ und λ wie folgt definiert ist:

$$\lambda(n) = \frac{\phi(n)}{\text{gcd}(p-1, q-1)}, \text{ wobei } \phi \text{ Eulersche } \phi - \text{ Funktion ist.}$$

Beweisen Sie, dass die Funktionen $e(x) \equiv x^b \mod n$ und $d(x) \equiv y^a \mod n$ zueinander inverse Funktionen sind.

(b) Bestimmen Sie d sowohl in RSA Konstruktion als auch in der im Teil (a) modifizierten Konstruktion für $n = 19939$ und $e = 203$.

(c) Ein Element $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ heßt fixiert, falls $e(x) \equiv x \mod n$ gilt, wobei die Funktionen wie im Teil (a) definert sind. Bestimmen Sie die Anzahl der fixierten Elemente in $(\mathbb{Z}/n\mathbb{Z})^\times$ für gegebenes n.

(5 Punkte)

3. Aufgabe

Argumentieren Sie, ob das RSA Kryptosystem unter chosen Chiffretext Angriff sicher ist.

(2 Punkte)

4. Aufgabe

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 $(\gcd(g, h)) = 1$ ist.

(a) Argumentieren Sie, warum der euklidische Algorithmus in R nicht immer funktionieren kann.

(b) Geben Sie ein Gegenbeispiel an, wo der euklidische Algorithmus in R fehlschlägt.

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

(5 Punkte)

5. Aufgabe

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 **Factoris ation** (zum Faktorisieren von ganzen Zahlen).

(6 Punkte)