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: 14.12.2007
in der Übung

8. Übung Kryptographie

(RSA-Sicherheit, Rabin, Blum-Goldwasser und Goldawasser-Mikali Kryptosysteme)

---

1. Aufgabe

(a) 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, dass für ein solches k folgendes gilt:

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

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

(b) Berechnen Sie die folgenden Ausdrücke und schreiben Sie dabei jeden einzelnen Rechenschritt auf:

- $\left(\frac{4628}{6409}\right)$
- $\left(\frac{873475982374598}{8085}\right)$

(5 Punkte)

2. Aufgabe

(a) Argumentieren Sie, ob das Rabin Kryptosystem bezüglich chosen ciphertext Angriff sicher ist.

(b) Wir wissen, dass die Entschlüsselungsfunktion des Rabin Kryptosystems keinen eindeutigen Klartext findet. Wie können wir das System so abändern, damit wir eine eindeutige Entschlüsselung ermöglichen können?

(c) Ist dieses geänderte Verfahren unter chosen ciphertext Angriff sicher?

(4 Punkte)

3. Aufgabe

Seien p eine ungerade Primzahl mit $p \equiv 5 \mod 8$ und a ein quadratischer Rest modulo p. Zeigen Sie, dass entweder $\pm a^{(p+3)/8}$ modulo p oder $\pm 2a(4a)^{(p-5)/8}$ modulo p quadratische Wurzeln von a modulo p sind.

(3 Punkte)

4. Aufgabe

Wir haben in der Übung folgenden Algorithmus betrachtet um für eine ungerade Primzahl p und a mit $\left(\frac{a}{p}\right) = 1$ die quadratische Wurzeln von a zu bestimmen.

Eingabe: p und a.
Ausgabe: Zwei quadratische Wurzeln von a.

(a) Wähle zufälliges b mit $\left(\frac{b}{p}\right) = -1$.

(b) Finde $p - 1 = 2^s t$ mit $\gcd(2, t) = 1$.

(c) Setze $c \to b^t \mod p$ und $r \to a^{(t+1)/2} \mod p$.

(d) For i from 1 to $s - 1$ do

- Berechne $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \mod p$.
- Setze $r \to r \cdot c \mod p$, falls $d \equiv -1 \mod p$ ist.
- Setze $c \to c^2 \mod p$.

(e) Return$(r, -r)$.

- Zeigen Sie, dass der Algorithmus korrekt ist.
- Argumentieren Sie, ob der Algorithmus die quadratischen Wurzeln von einem quadratischen Rest a modulo n finden kann, falls wir anstatt die Primzahl p den RSA-Modul $n = pq$ eingeben.

(5 Punkte)

5. Aufgabe

Implementieren Sie die Verschlüsselungs- und Entschlüsselungverfahren des Rabin Kryptosystems. Die besonderen Fälle $p, q \equiv 3 \mod 8$ und $p, q \equiv 5 \mod 8$ (Aufgabe 3) muss man bei der Implementierung betrachten.

(6 Punkte)

Hinweis: Die Aufgabe 5 kann bis 20.12.2007 abgegeben werden.