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

8. 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 Faktorisierung des RSA-Moduls n bei gegebenem d (6 Punkte)

(i) Seien $a, n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$ und $n = pq$ ($p, q > 2$ prim und verschieden). Die Verschlüsselungs- und Entschlüsselungsexponenten seien mit e und d bezeichnet. Ferner sei $ed - 1 = k \cdot 2^s$ mit $s \in \mathbb{N} \cup \{0\}$ maximal. Zeigen Sie, daß wenn die Ordnung von $a^k \mod p$ von der von $a^k \mod q$ verschieden ist gilt:

$$1 < \mathrm{ggT}(a^{2^t k} - 1, n) < n$$

für ein $t \in \{0, 1, ..., s-1\}$.

(ii) Zeigen Sie, daß die Anzahl der zu n primen Zahlen a in der Menge $\{1, ..., n-1\}$ für die $a^k \mod p$ und $a^k \mod q$ eine verschiedene Ordnung hat größer oder gleich $(p-1)(q-1)/2$ ist.

(iii) Sei $n = 253, e = 3$ und $d = 147$. Berechnen Sie p und q mit Hilfe von (i) und (ii) die Elemente p und q von n.

3. Aufgabe Praktische Aufgabe: OAEP (10 Punkte)

(i) Schreiben Sie in KASH einen sogenannten RSA-Pesudo-Zufallsgenerator. Sie finden eine Beschreibung eines Algorithmus z.B. in "Handbook of applied cryptography" Kapitel 5, Abschnitt 5.5.1: "RSA pseudorandom bit generator" auf der Kryptographie-Homepage.

(ii) Auf der Kryptographie-Homepage befindet sich eine Datei "OAEP". Diese enthält eine Hashfunktion. In Folgendem soll das OAEP-Verfahren implementiert werden (Optimal Asymetric Encription Padding). Dabei soll G ein Pseudo-Zufallsgenerator, h eine Hashfunktion und f eine Verschlüsselungsfunktion bezeichnen mit

$$f : D \longrightarrow D, \quad D \subseteq \{0,1\}^n,$$

$$G : \{0,1\}^k \longrightarrow \{0,1\}^l,$$

und

$$h : \{0,1\}^l \longrightarrow \{0,1\}^k$$

wobei $n = k + l$ und $n, k, l \in \mathbb{N}$ ist.

Die Ver- und Enrschlüsselung im OAEP-Verfahren funktioniert folgendermaßen:

Verfahren zum Verschlüsseln:

Sei m die zu verschlüsselnde Nachricht.

(a) Wähle eine Zufallszahl $r \in \{0,1\}^k$

(b) Setze $x = (m \oplus G(r)) \circ (r \oplus h(m \oplus G(r))$

(c) Falls $x \notin D$ wiederhole das Verfahren bei (a)

(d) Verschlüsseln mit $c = f(x)$

Verfahren zum Entschlüsseln:

Sei c die zu entschlüsselnde Nachricht.

(a) Setze $x = f^{-1}(c)$

(b) Bestimme a, b mit $x = a \circ b$ und $|a| = l$ sowie $|b| = k$

(c) Bestimme $r = h(a) \oplus b$

(d) Bestimme $m = a \oplus G(r)$

Dabei soll $\circ$ die Konkatenation zweier Bit-Strings und $\oplus$ die Addition in $\mathbb{Z}/2\mathbb{Z}$ bedeuten. Schreiben Sie ein KASH-Programm, daß für eine vorgegebene Zahl $n = pq$ eine Nachricht mit dem RSA-OAEP-Verfahren ver- und entschlüsselt, d.h. die Verschlüsselungsfunktion f soll die des RSA-Verfahrens sein.

(iii) Welchen Sinn hat das Padding beim OAEP?

Schicken Sie Ihren **lauffähigen** KASH-Code an wagner@math.tu-berlin.de als **Attachement**. Benutzen Sie die vorgegebenen Funktionsnamen in der Datei "OAEP" auf der Kryptographie-Homepage.

Gesamt: 20 Punkte