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: 12.01.2007
in der Übung

9. Übung Kryptographie

(Primzahl- und Zerlegbarkeitstests)

---

1. Aufgabe

(a) Ein $n \in \mathbb{N}$ heißt **zusammengesetzt**, falls n nicht prim ist. Sei n eine zusammengesetzte ungerade Zahl für die

$$a^{n-1} \equiv 1 \mod n$$

gilt für ein $a \in \mathbb{Z}$. Solch eine Zahl nennt man **Pseudoprimzahl** zur Basis a. Ist n für alle $a \in \mathbb{Z}$ mit $\gcd(a, n) = 1$ eine Pseudoprimzahl zur Basis a, so nennt man n **Carmichael-Zahl**. Man nennt $n \in \mathbb{N}$ **quadratfrei**, wenn es kein $p \in \mathbb{P}$ gibt mit $p^2|n$. Zeigen Sie, dass eine Carmichael-Zahl mindestens drei verschiedene Primteiler hat.

Benutzen Sie dazu die folgende Aussage ohne Beweis:

$$n \text{ ist Carmichael-Zahl } \Leftrightarrow n \text{ ist quadratfrei und es gilt: } p|n \Rightarrow (p-1)|(n-1) \quad (p \in \mathbb{P}).$$

(b) Zeigen Sie, dass $N = 294409$ eine Carmichael-Zahl ist.

(c) Zeigen Sie ohne Benutzung der Aussage vom Teil (a), dass $M = (6k+1)(12k+1)(18k+1)$ eine Carmichael-Zahl ist, falls $6k+1, 12k+1, 18k+1 \in \mathbb{P}$ für $k \in \mathbb{N}$ sind.

(5 Punkte)

2. Aufgabe

(a) Seien $N \in \mathbb{N}$ und $N - 1 = \prod_{i=1}^{t} p_i^{e_i}$ die Primfaktorzerlegung von $N-1$. Beweisen Sie, dass N prim ist, falls es ein $a \in \mathbb{N}$ mit $a^{N-1} \equiv 1 \mod N$ und $a^{\frac{N-1}{p_i}} \not\equiv 1 \mod N$ für $1 \leq i \leq t$ existiert.

(b) Seien $N \in \mathbb{N}$ eine ungerade Zahl und $N - 1 = \prod_{i=1}^{t} p_i^{e_i}$ die Primfaktorzerlegung von $N-1$. Beweisen Sie, dass N prim ist, falls für $1 \leq i \leq t$ ein a_i mit $a_i^{N-1} \equiv 1 \mod N$ und $a_i^{\frac{N-1}{p_i}} \not\equiv 1 \mod N$ existiert.

(c) Zeigen Sie, dass die Zahl 246247 eine Primzahl ist.

(d) Zeigen Sie, dass $n = 2^k$ mit $k \in \mathbb{N}$ ist, falls $N = 2^n + 1$ eine Primzahl ist.

(e) Zeigen Sie, dass $n \in \mathbb{P}$ gilt, falls $N = 2^n - 1$ eine Primzahl ist. Gilt die Umkehrung dieser Aussage? Begründen Sie Ihre Antwort.

(7 Punkte)

3. Aufgabe

Ist p eine Primzahl und g ein Erzeuger der multiplikativen Gruppe $G := (\mathbb{Z}/p\mathbb{Z})^\times$, so berechnet man für ein $x \in \{0, 1, ..., p-2\}$ das Element $y = g^x$. Dieses y ist öffentlich wohingegen x privat ist. Ist nun $m \in G$ eine zu verschlüsselnde Nachricht, so wählt man $r \in \mathbb{Z}$ zufällig und bildet $u := g^r$ und $v := my^r$. Der Chiffretext ist dann (u, v). Zum Entschlüsseln berechnet man dann $vu^{-x} = my^r g^{-rx} = mg^{rx}g^{-rx} = m$. Dieses Kryptosystem heißt **ElGamal Kryptosystem**.

(a) Bestimmen sie alle Erzeuger von von $(\mathbb{Z}/43\mathbb{Z})^\times$.

(b) Alice erhält den ElGamal-Chiffretext $(u = 37, v = 24)$. Ihr öffentlicher Schlüssel ist $(p = 43, g = 3)$. Bestimmen Sie den zugehörigen Klartext, wenn $x = 9$ ist.

(c) Der öffentliche Schlüssel von Bob sei $p = 53, g = 2, y = 30$. Alice erzeugt damit den Chiffretext $(24, 37)$. Wie lautet der Klartext?

(4 Punkte)

4. Aufgabe

Implementieren Sie den Miller-Rabin-Test.

(5 Punkte)

Hinweis: Die Aufgabe 4 kann bis 12.01.2008 abgegeben werden.