TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 13.1.09
www.math.tu-berlin.de/~hess/krypto-ws2008

10. Übung Kryptographie

1. Aufgabe

Bei dieser Aufgabe soll gezeigt werden, dass beim Solovay-Strassen-Test für eine zusammengesetzte Zahl auch ein Zeuge existiert, der das belegt.

(a) Seien p und q ungerade natürliche Zahlen, $p \in \mathbb{P}$, q teilerfremd zu p und gelte $n = p^k q$ mit $k \geq 2$. Sei $a = 1 + p^{k-1}q$. Zeigen Sie:

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$$

(b) Sei $n = p_1 \dots p_s$ das Produkt verschiedener ungerader Primzahlen. Zeigen Sie, dass für ein Element a mit a ist quadratischer Nichtrest mod p_1 und $a \equiv 1 \mod p_2 \dots p_s$ gilt

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n.$$

Existiert solch ein a?

(c) Warum kann also der Solovay-Strassen-Test für jede zusammengesetzte Zahl einen Zeugen finden?

(7 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 alle i mit $1 \leq i \leq t$ existiert.

(b) 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 für alle $1 \leq i \leq t$ 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 falls $N = 2^n + 1$ eine Primzahl ist, dann ist n von der Form $n = 2^k$ mit $k \in \mathbb{N}$. eine Primzahl ist.

(6 Punkte)

3. Aufgabe

Beweisen Sie mit Lemma 9 und der anschließenden Bemerkung aus dem „Miller-Rabin Skript“, dass -1 und 1 die einzigen Nichtzeugen für die Zerlegbarkeit von 9 sind.

(3 Punkte)

4. Aufgabe

Programmiern Sie den Miller-Rabin Primzahltest und finden Sie die kleinste Primzahl, bei der fünf mal die Ziffer Drei auftaucht. **(4 Punkte)**