Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 28.11.2013

Wintersemester 2013/14

Elementare Zahlentheorie

Übungszettel 7

Aufgabe 32: Betrachten Sie das RSA-Verfahren. Ihr öffentlicher Schlüssel sei (n, s). Sie erhalten von der NSA eine verschlüsselte Botschaft $c \equiv m^s \pmod{n}$ mit der Bitte, diese zu entschlüsseln. Nehmen Sie an, Sie wissen sicher,

(a) dass die NSA keine ausreichenden Fähigkeiten hat, aus der Kenntnis von (n, s, c, m) den Wert d mit $ds \equiv 1 \pmod{\varphi(n)}$ zu berechnen;

(b) dass es sich bei c nicht um eine abgefangene Botschaft von jemand anderem handelt.

Spricht ein *mathematischer* Grund dagegen, der NSA die entschlüsselte Botschaft zu schicken? *Hinweis:* Auch $m = m_1 m_2$ ist eine Botschaft. **(3 Punkte)**

Aufgabe 33: Dieselbe Botschaft m werde zweimal mit dem RSA-Verfahren verschlüsselt, einmal mit (n, s_1) und einmal mit (n, s_2) – die RSA-Moduln sind also beide Male gleich. Zeigen Sie, dass man die Botschaft leicht entschlüsseln kann, wenn man c_1, c_2 kennt und s_1 und s_2 teilerfremd sind. **(3 Punkte)**

Aufgabe 34: Sei $n \in \mathbb{N}$ und $(q-1)^2 < n \leq q^2$. Zeigen Sie, dass man q in $O(\log(n))$ Schritten berechnen kann. **(3 Punkte)**

Aufgabe 35: Seien p, q zwei Primzahlen. Ist es schwierig, die Primzahlen p, q zu bestimmen, wenn man nur $n = pq$ und $\varphi(n)$ kennt? **(3 Punkte)**

Aufgabe 36: Zeigen Sie:

(a) Für jede Zahl $k \in \mathbb{Z}$ gilt: $(2k+1)^2 \equiv 1 \pmod{8}$.

(b) Seien $m, n \in \mathbb{N}$ und sei p eine Primzahl. Dann ist $m^p - n^p$ entweder zu p teilerfremd oder durch p^2 teilbar. **(2+3 Punkte)**

Abgabe bis zum 5.12.2013!