Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 19.1.2017

Wintersemester 2016/17

Diskrete Mathematik

Übungsblatt 12

Aufgabe 55: Lösen Sie das folgende System von Kongruenzen:

$$\begin{aligned} x &\equiv 5 \pmod 5 \\ x &\equiv 4 \pmod 6 \\ x &\equiv 3 \pmod 7. \end{aligned}$$

(4 Punkte)

Aufgabe 56: Lösen Sie das folgende System von Kongruenzen:

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 3x &\equiv 1 \pmod 5 \\ 5x &\equiv 1 \pmod{11}. \end{aligned}$$

(4 Punkte)

Aufgabe 57: Folgende Botschaft ist mit dem RSA-Verfahren verschlüsselt: 9424184 15241303 6729921. Der öffentliche Schlüssel ist $n = pq = 16062481, s = 4321$. Übernehmen Sie die Rolle eines Aggressors und entschlüsseln Sie die Botschaft. Dabei steht jeder Block für drei bis vier Buchstaben, wobei 01 für A steht, 02 für B, ... und 26 für Z.

Hinweis: Computereinsatz (z.B. Maple, Mathematica) ist ausdrücklich erlaubt. Geben Sie aber bitte keinen Programmcode ab, sondern beschreiben Sie, wie Sie vorgehen (Screenshots etc.). **(3 Punkte)**

Aufgabe 58: Seien p, q zwei Primzahlen. Ist es schwierig, die Primzahlen p, q zu bestimmen, wenn man nur $n = pq$ und $\varphi(n)$ kennt? **(2 Punkte)**

Aufgabe 59*: 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 die verschlüsselten Botschaften c_1, c_2 kennt und s_1 und s_2 teilerfremd sind. **(3 Bonuspunkte)**

Aufgabe 60:

(a) Zeigen Sie, dass zur Berechnung von a^{2^k} nicht mehr als k Multiplikationen notwendig sind.

(b) Sei $\mathrm{ggT}(a, n) = 1$. Wie kann man die Inverse $a^{-1} \pmod n$ effizient berechnen, wenn man $\varphi(n)$ bereits kennt? **(1+2 Punkte)**

Abgabe bis zum 26.1.2017!