Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

7. Übungsblatt

Abgabe: Mittwoch, 25.5.11

Aufgabe 1 *Der Chinese Sun-Tsu stellt in seinem Buch* Suan-Ching *u.a. folgende Aufgabe: Wir haben eine gewisse Anzahl von Dingen, wissen aber nicht genau wie viele. Wenn wir sie zu je drei zählen, bleiben zwei übrig. Wenn wir sie zu je fünf zählen, bleiben drei übrig. Wenn wir sie zu je sieben zählen, bleiben zwei übrig. Wieviele Dinge sind es?*

Aufgabe 2 *Seien $n_1, \ldots, n_r$ paarweise teilerfremde natürliche Zahlen und seien $a_1, \ldots, a_r$ beliebige ganze Zahlen. Nach dem chinesischen Restsatz gibt es eine ganze Zahl a so, dass gilt:*

$$a \equiv a_1 \bmod n_1, \ldots, a \equiv a_2 \bmod n_2.$$

Geben Sie eine Lösung a an und begründen Sie, warum diese Zahl eine Lösung ist. (Hinweis: Informieren Sie sich in der Literatur!).

Aufgabe 3 *Es seien $p = 123456791$, $q = 987654323$, $n = p \cdot q$ und $e = 127$. Der Klartext sei*

$$a = 14152019010605 \in \mathbb{Z}_n.$$

Berechnen Sie $a^e \bmod p$ und $a^e \bmod q$. Berechnen Sie hieraus mithilfe des chinesischen Restsatzes $c \equiv a^e \bmod n$.

Aufgabe 4 *Um eine Textnachricht mit RSA zu verschlüsseln, wandeln wir sie zunächst wie folgt in eine Zahlenfolge um: Der Klartext wird so eingeteilt, dass je zwei Buchstaben einen Block von vier Ziffern bilden:*

$$a = 00, b = 01, c = 02 \text{ usw..}$$

Zum Beispiel wird die Nachricht "klar" zu 1011 0017*. Diese Ziffernblöcke können dann mit RSA verschlüsselt werden.*

Es sei $(n, e) = (3149, 563)$ der öffentliche Schlüssel beim RSA Verfahren. Hiermit wurde der folgende Geheimtext erzeugt:

$$1263 \quad 0996 \quad 1102 \quad 3039 \quad 2177 \quad 2311.$$

Wie lautet der geheime Schlüssel d? Bestimmen Sie den Klartext.