*Kryptographie* *WS 2015/16*
*Barbara Baumeister*
*Tutoren: Apolonia Gottwald, Soeren Senkovic*

# 4. Übungsblatt

**Abgabe: Donnerstag, 19.11.2015**

**Aufgabe 1** *Common-Modulus-Attacke*: Eine Nachricht $m$ sei zweimal mit dem RSA-Verfahren verschlüsselt und zwar mit den öffentlichen Schlüsseln $(n, e)$ und $(n, f)$, wobei $e$ und $f$ teilerfremd sind.

(a) Wie kann man $m$ aus den beiden Schlüsseln $c_e \equiv m^e \pmod{n}$ und $c_f \equiv m^f \pmod{n}$ berechnen?

(b) Die Nachricht $m$ wurde mit den öffentlichen Schlüsseln $(493, 3)$ und $(493, 5)$ verschlüsselt. Die Chiffretexte sind 293 und 421. Verwende die Common-Modulus-Attacke, um $m$ zu bestimmen.

**Aufgabe 2** Sei $n = 1591$. Der öffentliche RSA-Schlüssel von Alice sei $(n, e)$, wobei $e$ minimal sei. Sie erhält die verschlüsselte Nachricht 1292. Dechiffriere diese Nachricht mit Hilfe des Satzes über simultane Kongruenzen.

**Aufgabe 3** Funktioniert das RSA-Verfahren auch, wenn $n = p_1p_2p_3$ Produkt dreier verschiedener Primzahlen $p_1, p_2$ und $p_3$ ist?

**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.