Kryptographie *WS 2012/13*
Barbara Baumeister

5. Übungsblatt

Abgabe: Donnerstag, 15.11.2012

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 $c_e \equiv m^e \bmod n$ und $c_f \equiv m^f \bmod n$ 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 Gib zwei Gründe an, warum die beiden Primzahlen bei der RSA-Verschlüsselung verschieden seien sollten.

Aufgabe 3 Funktioniert das RSA-Verfahren auch, wenn $n = p \cdot q \cdot r$ Produkt dreier verschiedener Primzahlen p, q und r ist?

Aufgabe 4 Sei $n = 1189$. Der öffentliche RSA-Schlüssel von Alice ist (n, e) mit minimalem e. Alice erhält die verschlüsselte Nachricht $c = 1062$. Entschlüsseln Sie diese Nachricht mit Hilfe des Satzes über simultane Kongruenzen.