Angewandte diskrete Mathematik

Wintersemester 2008/2009
Barbara Baumeister
Jürgen Schütz

Freie Universität Berlin
Institut für Mathematik

Aufgabenblatt 10

Ausgabe: 6.1.2009

Abgabe: 13.1.2009

Aufgabe 37. — 4 Punkte

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 Schlüsseltexten $c_e = m^e \mod n$ und $c_f = m^f \mod n$ 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 38. — 4 Punkte

Sei $n = 1591$. Der öffentliche Schlüssel von Alice sei (n, e), wobei e minimal ist. Sie erhält die verschlüsselte Nachricht 1292.

Dechiffriere diese Nachricht mit Hilfe des chinesischen Restsatzes.

Aufgabe 39. — 4 Punkte

Funktioniert das RSA-Verfahren auch, wenn $n = p_1 p_2 p_3$ Produkt dreier paarweise verschiedener Primzahlen p_1, p_2, p_3 ist?

Aufgabe 40. — 4 Punkte

Gib zwei Gründe an, warum die beiden Primzahlen bei der RSA-Verschlüsselung verschieden sein sollten.