Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 18.12.2015

Einführung in Kryptographie

WS 2015/2016

Präsenzübungszettel 5

AUFGABE 1:
Sei (N, e) ein öffentlicher RSA Schlüssel mit $N = pq$, p, q prim und ungerade, $e = 3$.

a) Zeigen Sie, dass für $a, b \in \mathbb{Z}$ gilt: $a = b \mod N$ genau dann wenn $a = b \mod p$ und $a = b \mod q$.

b) Zeigen Sie, dass es genau drei verschiedene Elemente $x \in \mathbb{Z}_p$ gibt, so dass $x^3 = x \mod p$ gilt.

c) Zeigen Sie mit Hilfe des chinesischen Restsatzes (Satz 6.8), dass es genau neun Nachrichten $m \in \mathbb{Z}_N = \mathcal{P}$ gibt mit $E_{(N,e)}(m) = m$.

AUFGABE 2:
Zeigen Sie: RSA ist nicht sicher gegen *Chosen-Ciphertext-Angriffe (CCA)*. Beschreiben Sie dazu einen effizienten CCA-Angreifer, der jeden gegebenen Chiffretext $c \in \mathbb{Z}_N$ entschlüsseln kann, wobei nur eine Entschlüsselungsanfrage für $c' \in \mathbb{Z}_N, c' \neq c$ ausgeführt wird.