RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae, Philipp Wagner, Vera Knüppels

Präsenzübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 5

AUFGABE 1:
Berechnen Sie $\varphi(11)$, $\varphi(64)$ und $\varphi(540)$.

AUFGABE 2:
Beweisen Sie $\varphi(n^2) = n\varphi(n)$.

AUFGABE 3:
Beweisen Sie die Korrektheit der Entschlüsselung des RSA-Kryptosystems. Beachten Sie, dass der Satz von Euler nur für jene Nachrichten m gilt, die teilerfremd zu $N = pq$ sind.

AUFGABE 4:
Alice, Bob und Charles verwenden den gleichen öffentlichen Schlüssel $e = 3$ für das RSA-Kryptosystem, aber unterschiedliche Moduli $N_1 = 51, N_2 = 65, N_3 = 77$. Alle drei Verschlüsseln die selbe Nachricht m und erhalten den Chiffretext $c_1 = 23, c_2 = 60, c_3 = 48$. Beschreiben Sie, wie Sie die Nachricht effizient berechnen können, ohne dabei die Faktorisierung von N_i zu benutzen. Welche Nachricht wurde verschlüsselt?