RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 1 / 13. Oktober 2010

AUFGABE 1:
Zeigen Sie, dass kein Public-Key Kryptosystem mit *deterministischer* Verschlüsselungsfunktion semantisch sicher ist.

AUFGABE 2:
Berechnen Sie mit Hilfe des Erweiterten Euklidischen Algorithmus das Inverse von 17 in $\mathbb{Z}_{23}^*$.

AUFGABE 3:
Gegeben sei ein RSA-Signierorakel, dass bei Eingabe $m' \neq m$ die RSA-Signatur von m' zurückliefert. Zeigen Sie, dass man dann effizient die Signatur von m berechnen kann, d.h. man kann RSA-Signaturen *universell* fälschen.

AUFGABE 4:
Bestimmen Sie die Ordnungen der multiplikativen Gruppen $\mathbb{Z}_{19}^*, \mathbb{Z}_{21}^*$ und $\mathbb{Z}_{27}^*$. Bestimmen Sie außerdem ord(2) in diesen Gruppen.

AUFGABE 5:
Sei $N = pq$ mit $p \neq q$ prim. Zeigen Sie, dass $\text{ord}(\mathbb{Z}_N^*) = (p-1)(q-1)$.

AUFGABE 6:
Finden Sie alle Lösungen der folgenden Gleichungen.

(a) $3x + 5 = 7 \bmod 8$

(b) $x^2 = 1 \bmod 8$