RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 1 / 16. Oktober 2012

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

AUFGABE 2:
Sei G eine endliche multiplikative Gruppe mit neutralem Element 1. Sei $a \in G$ beliebig. Zeigen Sie, dass $\langle a \rangle = \{a^1, a^2, \ldots, a^{\mathrm{ord}(a)}\}$ eine multiplikative Gruppe ist.

AUFGABE 3:
Berechnen Sie mit Hilfe des Erweiterten Euklidischen Algorithmus das Inverse von 13 in $\mathbb{Z}_{21}^*$.

AUFGABE 4:
Bestimmen Sie die Ordnungen der multiplikativen Gruppen $\mathbb{Z}_{15}^*, \mathbb{Z}_{17}^*$ und $\mathbb{Z}_{27}^*$. Bestimmen Sie außerdem ord(2) in diesen Gruppen.

AUFGABE 5:
Finden Sie alle Lösungen der folgenden Gleichungen.

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

(b) $x^2 = 1 \bmod 14$