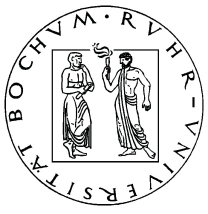
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 1 / 21. Oktober 2009

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

AUFGABE 2:
Finden Sie alle Lösungen der folgenden Gleichungen.

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

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

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

AUFGABE 5:
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 6:
Sei G eine 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.