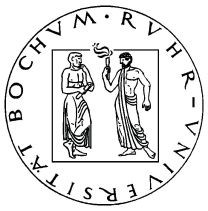
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen



Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 1 / 17. April 2008

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

AUFGABE 2:

(a) Finden Sie alle Lösungen der folgenden Gleichung.

$$5x + 2 \equiv 6 \pmod 9$$

(b) Berechnen Sie mit Hilfe des Erweiterten Euklidischen Algorithmus das Inverse von 8 in $\mathbb{Z}_{19}^*$.

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:

(a) Sei $N \in \mathbb{N}$. Zeigen Sie, dass $\mathbb{Z}_N^*$ eine multiplikative Gruppe ist.

(b) Sei $p \in \mathbb{N}$ prim. Zeigen Sie, dass $\varphi(p) := \text{ord}(\mathbb{Z}_p^*) = p - 1$.

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