RUHR UNIVERSITÄT BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 5 / 6.–8. Mai 2013

AUFGABE 1:
Zeigen Sie, dass für beliebige Zahlen $n \in \mathbb{Z}$ mit $n > 0$ stets gilt:
$\phi(n^2) = n\phi(n)$

AUFGABE 2:
Seien $p \neq q$ Primzahlen und $N := pq$. Sei $e > 0$ teilerfremd zu $\phi(N) = (p-1)(q-1)$.
Zeigen Sie:

(a) e ist teilerfremd zu $\mathrm{kgV}(p-1, q-1)$

(b) Sei d so gewählt, dass $d \cdot e \equiv 1 \mod \mathrm{kgV}(p-1, q-1)$. Zeigen Sie, dass dann für beliebige $a \in \mathbb{Z}_N^*$ gilt: $a^{ed} \equiv a \mod N$.

Bemerkung: Obige Gleichung gilt (wie auch bei normalem RSA) auch für alle $a \in \mathbb{Z}_N$. Beachte, dass $\mathrm{kgV}(p-1, q-1) < \phi(N)$, falls p, q ungerade.

AUFGABE 3:
Geben Sie alle irreduziblen Polynome vom Grad ≤ 4 in $\mathbb{F}_2[X]$ an.

AUFGABE 4:
Geben Sie eine Multiplikationstabelle und eine Additionstabelle für $\mathbb{Z}/4\mathbb{Z}$ und für $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$

AUFGABE 5:
Zeigen Sie, dass die Gruppe $(\mathbb{F}_p[X], +)$ nicht endlich erzeugt ist.

AUFGABE 6:

(a) Geben Sie alle $n \in \mathbb{N}$ an mit $\phi(n) = \frac{n}{2}$

(b) Geben Sie alle $n \in \mathbb{N}$ an mit $\phi(2n) = \phi(n)$

Hinweis zu (a): Betrachten Sie den größten Primfaktor von n.

AUFGABE 7:
Seien (N_1, e_1), (N_2, e_2), (N_3, e_3) die öffentliche RSA-Schlüssel mit paarweise teilerfremden N_i und jeweils $e_1 = e_2 = e_3 = 3$ von 3 Personen, die zufälligerweise alle Bob heißen. Alice möchte

nun eine Nachricht $m \in \mathbb{Z}, 0 \leq m < N$ an Bob schicken. Da sie sich nicht sicher ist, welcher Bob der richtige Empfänger ist, schickt sie die selbe Nachricht kurzerhand an alle 3 Bobs, (naiv) verschlüsselt zu jeweils $c_i = m^{e_i} \bmod N_i$.
Überlegen Sie sich, wie man den Klartext m effizient berechnen kann, wenn man alle 3 gesendeten verschlüsselten Nachrichten c_1, c_2, c_3 abfängt.