Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie II

SS 2012

Blatt 5 / 13. Juni 2012 / Abgabe **bis spätestens Mittwoch, 27.06.2012 10:00 Uhr**

AUFGABE 1:

Sei $N > 1$ eine ungerade ganze Zahl, für die $\phi(N)$ und N teilerfremd sind. Wir wollen zeigen, dass die Gruppe $(\mathbb{Z}_{N^3}^*, \cdot)$ isomorph ist zu $(\mathbb{Z}_{N^2}, +) \times (\mathbb{Z}_N^*, \cdot)$. Zeigen Sie hierfür:

(a) $\phi(N^3) = N^2 \cdot \phi(N)$ [1 Punkt]

(b) $1 + N$ hat Ordnung N^2 in $\mathbb{Z}_{N^3}^*$ [2.5 Punkte]

(c) $\psi : \mathbb{Z}_{N^2} \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^3}^*, (a, b) \mapsto (1 + N)^a \cdot b^{(N^2)} \bmod N^3$ ist ein wohldefinierter Gruppenisomorphismus. [3.5 Punkte]

Bemerkungen/Hinweise: Gehen Sie den analogen Beweis für N^2 aus der Vorlesung durch und wiederholen Sie diesen. Teil (b) wird erheblich einfacher, wenn man die resultierende Gleichung erstmal modulo N^2 betrachtet und damit zeigt, dass die Ordnung ein Vielfaches von N sein muss. Mit wohldefiniert in (c) ist gemeint, dass $\psi(a, b)$ nur von $(a \bmod N^2)$ bzw. $(b \bmod N)$ abhängt statt von a, b.

AUFGABE 2:

Sei N eine Blum-Zahl, d.h. $N = pq$ mit $p \neq q$ prim, $p \equiv q \equiv 3 \bmod 4$.

Sei $A_N := \{x \in \mathbb{Z}_N^* \mid x < \frac{N}{2}, \left(\frac{x}{N}\right) = 1\}$.
Wir definieren $f_N : A_N \to A_N$ durch

$$f_N(x) = \begin{cases} x^2 \bmod N & \text{falls } x^2 \bmod N < \frac{N}{2} \\ (-x^2) \bmod N & \text{falls } x^2 \bmod N > \frac{N}{2} \end{cases}$$

Dabei wird bei Reduktion modulo N immer der Repräsentant zwischen 0 und $N-1$ gewählt.

(a) Zeigen Sie, dass f_N eine Permutation auf A_N ist. [2 Punkte]

(b) Konstruieren Sie hiermit eine Trapdoor-Einwegpermutation und beweisen Sie deren Einwegeigenschaft unter der Faktorisierungsannahme (für Blumzahlen). [5 Punkte]

AUFGABE 3:

Sei $f : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*$ der Isomorphismus aus der Vorlesung.
Für festes $c \in \mathbb{Z}_N^*$ sei $A_c := f(\{(x, c) \mid x \in \mathbb{Z}_{N^2}\})$.
Zeigen Sie, dass man bei gegebenem RSA-Modulus $N = pq$ unbekannter Faktorisierung und jedem fest gewähltem bekannten c, die Verteilung $z \in_R A_c$ in Polynomialzeit von $z \in_R \mathbb{Z}_{N^2}^*$ unterscheiden kann. [2 Punkte]

Bemerkung: Dies steht im Gegensatz zu $f(\{(c, x) \mid x \in \mathbb{Z}_N^*\})$, für welches dies nach DCR-Annahme nicht möglich ist.

AUFGABE 4:

(Bonusaufgabe) [4 Bonuspunkte]
Sei GenModulus ein Algorithmus, der Produkte $N = pqr$ von genau 3 verschiedenen Primzahlen ausgibt.
Zeigen Sie, dass das Berechnen von Quadratwurzeln bzgl. GenModulus hart ist, wenn das Problem der *vollständigen* Faktorisierung (d.h. Berechnen von p, q, r aus N) hart ist bzgl. GenModulus.

Bemerkung: Die Schwierigkeit dieser Aufgabe liegt in der sauberen formalen Analyse. Sie werden in Ihrer Reduktion den Algorithmus zum Berechnen von Quadratwurzeln mehrmals aufrufen müssen. Diese Aufrufe sind *nicht* unabhängig, da sie das selbe N benutzen. Daher darf man die Erfolgswahrscheinlichkeiten nicht ohne weitere Begründung einfach multiplizieren. Zudem sollte man sich überlegen, mit welcher Wahrscheinlichkeit man durch mehrmalige Aufrufe des Quadratwurzelalgorithmus einen neuen Primfaktor von N bekommt (und nicht etwa jedes mal den selben Primfaktor).