Übungen zur Kryptologie 1 Wintersemester 07/08

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 13

Aufgabe 61 (mündlich)

Eine ungerade zusammengesetzte Zahl n heißt stark pseudoprim zu einer Basis $a \in \mathbb{Z}_n^*$, falls der Miller-Rabin-Test diese Zahl bei Wahl der Basis a als prim klassifiziert (n ist also genau dann stark pseudoprim zur Basis a, wenn $a \in \mathcal{P}_n^{MRT}$ ist).
Zeigen Sie, dass die Zahl $n_1 = 3215031751$ stark pseudoprim zu jeder der Basen $2, 3, 5, 7$ ist. (Tatsächlich ist dies die einzige Zahl $n < 2,5 \cdot 10^{10}$ mit dieser Eigenschaft.)

Aufgabe 62 (mündlich)

Betrachten Sie folgendes Zufallsexperiment:

> Ein probabilistischer Primzahltest T (mit einseitiger Fehlerwahrscheinlichkeit ε im Fall einer zusammengesetzten Eingabe) wird auf eine zufällig gewählte ungerade Binärzahl $n \in [2^l, 2^{l+1} - 1]$ angewandt.

Bestimmen Sie näherungsweise die Wahrscheinlichkeiten der beiden Ereignisse "n ist prim" (Ereignis A) und "$T(n)$ gibt prim aus" (Ereignis B). Wie groß sind die bedingten Wahrscheinlichkeiten $\Pr[A/B]$ und $\Pr[B/A]$ im Fall $\varepsilon = 2^{-m}$, $m = 1, 2, 5, 10, 20, 30, 50, 100$? Interpretieren Sie diese Zahlen.

Aufgabe 63 (mündlich)

Zeigen Sie, dass ein Public-Key Kryptosystem nicht absolut sicher sein kann.

Aufgabe 64 (mündlich)

Zwei RSA-Exponenten $e_1, e_2 \in \mathbb{Z}_{\varphi(n)}^*$ heißen äquivalent, wenn für alle $x \in \mathbb{Z}_n$ gilt: $x^{e_1} \equiv_n x^{e_2}$.

a) Zeigen Sie, dass zwei RSA-Exponenten e_1 und e_2 genau dann äquivalent sind, wenn $e_1 \equiv_v e_2$ gilt, wobei $v = \mathrm{kgV}(p-1, q-1)$ und $n = pq$ die Primfaktorzerlegung von n ist.

b) Folgern Sie, dass der Entschlüsselungsexponent d aus e auch über die Kongruenz $ed \equiv_v 1$ bestimmt werden kann.

Aufgabe 65 (mündlich)

Ein RSA-Klartext $x \in \mathbb{Z}_n$ heiße Fixpunkt für den RSA-Exponenten e, wenn $x^e \equiv_n x$ ist. Bestimmen Sie die Anzahl der Fixpunkte in Abhängigkeit von e und n.

Aufgabe 66 (mündlich)

Sei A ein effizienter Algorithmus, der einen zufällig gewählten RSA-Kryptotext $y \in \mathbb{Z}_n$ mit Wahrscheinlichkeit $\varepsilon > 0$ dechiffriert. Transformieren Sie A in einen effizienten probabilistischen Algorithmus B, der jeden RSA-Kryptotext $y \in \mathbb{Z}_n$ bei Eingabe von y und einer Binärzahl $a \in \mathbb{N}$ mit Wahrscheinlichkeit $1 - 1/a$ dechiffriert.

Aufgabe 67 (schriftlich, 10 Punkte)

a) Verschlüsseln Sie den Klartext $x = 444$ mit dem RSA-Verfahren und dem öffentlichen Schlüssel $k = (613, 989)$.

b) Entschlüsseln Sie den Kryptotext $y = 444$, d. h. bestimmen Sie den Klartext x, für den gilt $E(k, x) = 444$.

c) Faktorisieren Sie die Zahl $n = 9382619383$ mit dem Verfahren der Differenz der Quadrate.

d) Faktorisieren Sie die Zahl $n = 4386607$ bei Kenntnis von $\varphi(n) = 4382136$.