Übungen zur Kryptologie 1 Wintersemester 05/06
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 13

Aufgabe 50 (mündlich)

Zeigen Sie, dass für jede Primzahlpotenz p^k die Kongruenz $x^2 \equiv_{p^k} 1$ genau zwei Lösungen $\pm a$ besitzt. *Hinweis:* p kann nicht $a+1$ und $a-1$ teilen.

Aufgabe 51 (mündlich)

Zeigen Sie:

a) Primzahlpotenzen p^k sind keine Carmichaelzahlen.
Hinweis: Berechnen Sie $(p^{k-1}+1)^{p^k-1} \bmod p^k$.

b) Jede Carmichaelzahl n ist quadratfrei.

c) Eine ungerade, zusammengesetzte und quadratfreie Zahl n ist genau dann eine Carmichaelzahl, wenn $p-1$ für jeden Primteiler p von n die Zahl $n-1$ teilt.

d) Jede Carmichaelzahl n lässt sich in drei teilerfremde Faktoren $n_1, n_2, n_3 > 1$ zerlegen.

e) 561, 2465, 1729, 172081, 294409 und 56052361 sind Carmichaelzahlen.

Aufgabe 52 (mündlich)

a) Sei $n > 2$ ungerade und sei $n-1 = 2^m u$, u ungerade. Weiter sei

$$J_n = \{a \in \mathbb{Z}_n^* \mid a^{2^j u} \equiv_n \pm 1\}, \text{ wobei } j = \max\{0 \le i \le m \mid \exists a \in \mathbb{Z}_n^* : a^{2^i u} \equiv_n -1\}.$$

Zeigen Sie, dass J_n eine Untergruppe von $\mathbb{Z}_n^*$ ist und die Menge

$$\mathcal{P}_n^{MRT} = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv_n 1 \text{ und } \forall i = 1, \dots m : a^{2^i u} \equiv_n 1 \to a^{2^{i-1} u} \equiv_n \pm 1\}$$

aller Primzahlzeugen des Miller-Rabin-Tests enthält.

b) Sei nun $n = n_1 n_2$ eine Carmichaelzahl mit teilerfremden Faktoren $n_1, n_2 > 1$. Zeigen Sie, dass für ein beliebiges $v \in J$ mit $v^{2^j u} \equiv_n -1$ die Zahl $w \in \mathbb{Z}_n^*$ mit

$$w \equiv_{n_1} v,$$
$$w \equiv_{n_2} 1$$

nicht in J enthalten ist. Schließen Sie hieraus, dass die Fehlerwahrscheinlichkeit beim Miller-Rabin-Test $\le 1/2$ ist.

Aufgabe 53 (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 $Prob[A/B]$ und $Prob[B/A]$ im Fall $\varepsilon = 2^{-m}$, $m = 1, 2, 5, 10, 20, 30, 50, 100$? Interpretieren Sie diese Zahlen.

Aufgabe 54 (mündlich)

Ein RSA-Exponent $e \in \mathbb{Z}^*_{\varphi(n)}$ heiße schwach, wenn für alle $x \in \mathbb{Z}_n$ gilt: $x^e \equiv_n x$. Zeigen Sie, dass für jeden RSA-Modul $n = pq$ genau $\varphi(n)/kgV(p-1, q-1) \geq 2$ verschiedene schwache RSA-Exponenten existieren. Wie können diese erkannt bzw. wie kann ihre Verwendung ausgeschlossen werden?

Aufgabe 55 (schriftlich, 10 Punkte)

a) 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.)

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

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

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

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