Übungen zur Kryptologie 1 Wintersemester 07/08

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 12

Aufgabe 54 (schriftlich, 10 Punkte)

Sei R der Polynom-Restklassenring $\mathbb{F}_{2^8}[y]/(y^4+1)$.

a) Zeigen Sie, dass R kein Körper ist.

b) Ist das Ringelement $a(y) = 03y^3 + 01y^2 + 01y + 02$ in R invertierbar? Bestimmen Sie gegebenenfalls das multiplikative Inverse $a^{-1}(y)$ von $a(y)$ in R.

c) Zeigen Sie, dass die AES-Operation MIXCOLUMNS eine multiplikative Chiffre mit festem Schlüssel $a(y)$ im Ring R realisiert.

Aufgabe 55 (mündlich)

Berechnen Sie $\varphi(75\,600)$, $\varphi(14\,948)$, $\log_{7,3} 4$, $\log_{37,2} 3$, $\mathrm{ord}_7(2)$ und $\mathrm{ord}_{31}(2)$.

Aufgabe 56 (mündlich)

Seien $m_1, \ldots, m_{n+1} \in \mathbb{N}$. Sei $g_i = \mathrm{ggT}(m_i, m_{n+1})$, $i = 1, \ldots, n$. Zeigen Sie

$$\mathrm{kgV}(g_1, \ldots, g_n) = \mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_n), m_{n+1}).$$

Aufgabe 57 (mündlich)

Betrachten Sie für $a_1, \ldots, a_n \in \mathbb{Z}$ und $m_1, \ldots, m_n \in \mathbb{N}$ folgendes System von linearen Kongruenzen

$$x \equiv_{m_i} a_i, \quad i = 1, \ldots n. \qquad (*)$$

a) Zeigen Sie, dass das Kongruenzgleichungssystem $(*)$ höchstens eine Lösung modulo $\mathrm{kgV}(m_1, \ldots, m_n)$ hat.

b) Zeigen Sie, dass das System $(*)$ genau dann lösbar ist, wenn für alle $1 \le i < j \le n$ die Zahl $\mathrm{ggT}(m_i, m_j)$ ein Teiler von $(a_i - a_j)$ ist.

Hinweis: Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 56.

Aufgabe 58 (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 59 (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

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

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 60 (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 $\varphi(n)/kgV(p-1, q-1) \ge 2$ verschiedene schwache RSA-Exponenten existieren. Wie können diese erkannt bzw. wie kann ihre Verwendung ausgeschlossen werden?