Übungen zur Kryptologie 1 Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 12

Aufgabe 42

Zeigen Sie, dass das System von linearen Kongruenzen

$$x \equiv a_i \pmod{m_i} \quad i = 1, \ldots n$$

genau dann lösbar ist, wenn $\mathrm{ggT}(m_i, m_j) | (a_i - a_j)$ für alle Paare (i, j) mit $1 \leq i < j \leq n$. Zeigen Sie: wenn eine Lösung existiert, dann ist sie eindeutig modulo $\mathrm{kgV}(m_1, m_2, \ldots, m_n)$.
Hinweis: Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 41.

Aufgabe 43

Sei a ein Element von $\mathbb{Z}_m^*$ der Ordnung $\mathrm{ord}_m(a) = k$. Zeigen Sie

$$\mathrm{ord}_m(a^i) = \frac{k}{\mathrm{ggT}(k, i)}.$$

Aufgabe 44

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 45 (schriftlich, 10 Punkte)

a) Verschlüsseln Sie den Klartext $x = 444$ nach dem RSA-Verfahren, falls $e = 613$ und $n = 989$ ist.

b) Entschlüsseln Sie den Kryptotext $y = 444$, d. h. bestimmen Sie den Klartext x, für den gilt $E_{(613,989)}(x) = 444$.

Abgabe am 13.2.2004