Wolfgang K. Seiler
Tel. 2515

A5, C201

9. November 2016

8. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

p sei eine Primzahl und $p \equiv 3 \bmod 4$.

a) Zeigen Sie: Falls die Kongruenz $x^2 \equiv a \bmod p$ eine Lösung hat, ist $y = a^{(p+1)/4}$ eine solche Lösung.

b) Falls die Kongruenz $x^2 \equiv a \bmod p$ keine Lösung hat, erfüllt $y = a^{(p+1)/4}$ die Kongruenz $y^2 \equiv -a \bmod p$.

c) Die Kongruenz $x^2 \equiv -1 \bmod p$ hat keine Lösung.

Aufgabe 2: *(3 Punkte)*

a) Bestimmen Sie alle Lösungen der Kongruenzen

$$x^2 \equiv 1 \bmod 15 \quad \text{und} \quad x^2 \equiv 4 \bmod 15\,!$$

b) Für welche $a \in \mathbb{Z}/15$ hat die Kongruenz $x^2 \equiv a \bmod 15$ eine Lösung, und wie viele Lösungen gibt es jeweils?

Aufgabe 3: *(7 Punkte)*

Faktorisieren Sie die Zahl $N = 851$ mit dem quadratischen Sieb mit Hilfe der Faktorbasis $\mathcal{B} = \{2, 5, 11, 17, 23\}$ und dem Siebintervall $[1, 40]$!

Aufgabe 4: *(5 Punkte)*

p sei eine Primzahl und $\mathbb{Z}/p^\times$ bezeichne die Menge $\{1, \ldots, p-1$ mit der Multiplikation modulo p als Verknüpfung.

a) Zeigen Sie; Die Abbildung

$$\varphi: \begin{cases} \mathbb{Z}/(p-1) \to \mathbb{Z}/p^\times \\ \qquad x \mapsto a^x \end{cases}$$

ist für jedes $a \in \mathbb{Z}/p^\times$ ein Homomorphismus, d.h. $\varphi(x+y) = \varphi(x) \cdot \varphi(y)$.

b) Für welche a ist φ im Falle $p = 11$ bijektiv?

c) Berechnen Sie die Tabelle der diskreten Logarithmen modulo elf zur Basis zwei!

Abgabe bis zum Dienstag, dem 15. November 2016, um 15.25 Uhr