Prof. J. Rothe Düsseldorf, 27.10.2009

Übung zur Vorlesung
Kryptologie 2

Blatt 3, Abgabe: 05.11.2009 bis 15:00 Uhr

Aufgabe 1 (5 Punkte): Führen Sie das Schlüsseltauschprotokoll von Diffie und Hellman konkret mit den Werten

- $p = 4079$,
- $\gamma = 1709$,
- $a = 2344$ und
- $b = 3420$

durch. Geben Sie bei jeder berechneten Zahl an, ob diese geheim oder öffentlich ist.

Aufgabe 2 (10 Punkte): Berechnen Sie in $\mathbb{Z}_{13}^*$, $\mathbb{Z}_{23}^*$ und $\mathbb{Z}_{33}^*$ jeweils alle primitiven Elemente.

Aufgabe 3 (15 Punkte): Berechnen Sie mit dem Algorithmus von Shanks

$$\begin{aligned} a &= \log_3 27 \mod 31, \\ b &= \log_3 267 \mod 401. \end{aligned}$$

Aufgabe 4 (freiwillig): Lösen Sie das Kongruenzensystem

$$\begin{aligned} 12 \cdot x &\equiv 13 \mod 29 \\ 7 \cdot x &\equiv 5 \mod 17 \end{aligned}$$

mit dem chinesischen Restesatz.

Aufgabe 5 (freiwillig): Bestimmen Sie alle primitiven Elemente von $\mathbb{Z}_{401}^*$.