Einführung in Kryptographie und Datensicherheit Übung 2

Tilman Bender Matrikelnummer: 108011247244

29. Oktober 2011

Aufgabe 1

a)

$$13 * 24 \equiv 22 \mod 29 \quad \text{(i)}$$

$$\begin{aligned} 17 * 1337 &\mod 29 \\ 17 * 3 \equiv 22 &\mod 29 \end{aligned} \quad \text{(ii)}$$

$$\begin{aligned} 69 * 31 &\mod 29 \\ 11 * 2 \equiv 22 &\mod 29 \end{aligned} \quad \text{(iii)}$$

$$\begin{aligned} (-36) * (-28) &\mod 29 \\ 22 * 1 \equiv 22 &\mod 29 \end{aligned} \quad \text{(iv)}$$

$$\begin{aligned} 231 * (-51) &\mod 29 \\ -1 * 7 \equiv 22 &\mod 29 \end{aligned} \quad \text{(v)}$$

b)

In allen fünf Fällen können die Multiplikationen vereinfacht werden indem man kleinere Faktoren aus der gleichen Äquivalenzklasse verwendet.

c)

$$3 * 3^{-1} \equiv 1 \Rightarrow 3^{-1} \equiv 10 \mod 29 \quad \text{(i)}$$

$$\begin{aligned} 6 * 6^{-1} \equiv 1 \Rightarrow 6^{-1} &\equiv 4 \mod 23 \\ \Rightarrow 2 * 6^{-1} &\equiv 8 \mod 23 \end{aligned} \quad \text{(ii)}$$

$$\begin{aligned} 3 * 3^{-1} \equiv 1 \Rightarrow 3^{-1} &\equiv 9 \mod 13 \\ 9 * 9^{-1} \equiv 1 \Rightarrow 9^{-1} &\equiv 3 \mod 13 \\ \Rightarrow 7 * 3 - 1 * 4 * 9^{-1} &\equiv 2 \mod 13 \end{aligned} \quad \text{(iii)}$$