Rasmus Diederichsen
Lisa Goerke
Sebastian Höffner

Sven Kleine-Albers
Kristin Schmidt

Lösungen zu Übungsblatt 6
Kryptographische Verfahren

Besprechung 11. Dezember 2015

Aufgabe 6.1. Exponentiation von Hand

a)

$$\begin{aligned}
\left[3^{1000}\right]_{100} &= \left[3^{512+256+128+64+32+8}\right]_{100} \\
&= \left[\left[\left[\left[\left[\left[3^{512}\right]_{100} \cdot 3^{256}\right]_{100} \cdot 3^{128}\right]_{100} \cdot 3^{64}\right]_{100} \cdot 3^{32}\right]_{100} \cdot 3^{8}\right]_{100} \\
&= \left[\left[\left[\left[41 \cdot 21\right]_{100} \cdot 61\right]_{100} \cdot 81\right]_{100} \cdot 41\right]_{100} \cdot 61\Big]_{100} \\
&= \left[\left[\left[\left[1 \cdot 61\right]_{100} \cdot 81\right]_{100} \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[\left[\left[61 \cdot 81\right]_{100} \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[\left[41 \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[81 \cdot 61\right]_{100} \\
&= 41
\end{aligned}$$

Nebenrechnungen:

$$\begin{aligned}
\left[3^{1}\right]_{100} &= 3 \\
\left[3^{2}\right]_{100} &= 9 \\
\left[3^{4}\right]_{100} &= \left[3^{2+2}\right]_{100} = \left[\left[3^{2}\right]_{100} \cdot 3^{2}\right]_{100} = \left[9 \cdot 3^{2}\right]_{100} = 81 \\
\left[3^{8}\right]_{100} &= \left[3^{4+4}\right]_{100} = \left[81 \cdot 3^{4}\right]_{100} = \left[6561\right]_{100} = 61 \\
\left[3^{16}\right]_{100} &= \left[3^{8+8}\right]_{100} = \left[3721\right]_{100} = 21 \\
\left[3^{32}\right]_{100} &= \left[441\right]_{100} = 41 \\
\left[3^{64}\right]_{100} &= \left[1681\right]_{100} = 81 \\
\left[3^{128}\right]_{100} &= 61 \\
\left[3^{256}\right]_{100} &= 21 \\
\left[3^{512}\right]_{100} &= 41 \\
\left[3^{1024}\right]_{100} &= 81 \\
&\vdots
\end{aligned}$$

Wir beobachten die Periode $81, 61, 21, 41, \ldots$, die wir uns zu Nutzen machen können.

b)

$$\begin{aligned}
\left[101^{4800000002}\right]_{35} &= \left[\left[16^{6}\right]_{35} \cdot \left[11^{5}\right]_{35}\right]_{35} \\
&= \left[11^{5}\right]_{35} \\
&= 16
\end{aligned}$$

Nebenrechnungen:

$$\begin{aligned}\left[101^1\right]_{35} &= 31\\ \left[101^2\right]_{35} &= 16\\ \left[101^4\right]_{35} &= 11\\ \left[101^8\right]_{35} &= 16\\ \left[101^{16}\right]_{35} &= 11\\ &\vdots\end{aligned}$$

Wir beobachten, dass jede zweite dieser Potenzen (also $2, 8, 32, \dots$) einen Rest von 16 hat, alle anderen (mit Ausnahme von 1) den Rest von 11. Mit diesem Wissen können wir mit der Binärdarstellung ein einfachem Zählen zu herausfinden, wie oft wir 11 bzw. 16 multiplizieren müssen, um auf das Ergebnis zu kommen:

$$4800000002_{10} = 100011110000110100011000000000010_2$$

Wir finden sechs Potenzen deren Rest 16 ist und fünf Potenzen deren Rest 11 ist. Es folgt:

$$\left[101^{4800000002}\right]_{35} = \left[\left[16^6\right]_{35} \cdot \left[11^5\right]_{35}\right]_{35}$$

Wir können nun zunächst $\left[16^6\right]_{35}$ geschickt berechnen:

$$\begin{aligned}\left[16^6\right]_{35} &= \left[16^{2+2+2}\right]_{35}\\ &= \left[11 \cdot 11 \cdot 11\right]_{35}\\ &= 1\end{aligned}$$

Wir stellen fest, dass wir diese Erkenntnis widerum in unsere Gleichung einsetzen können und erhalten:

$$\begin{aligned}\left[\left[16^6\right]_{35} \cdot \left[11^5\right]_{35}\right]_{35} &= \left[1 \cdot \left[11^5\right]_{35}\right]_{35}\\ &= \left[11^5\right]_{35}\end{aligned}$$

Das können wir erneut geschickt berechnen:

$$\begin{aligned}\left[11^5\right]_{35} &= \left[11^{4+1}\right]_{35}\\ &= \left[11 \cdot 11\right]_{35}\\ &= 16\end{aligned}$$

Nebenrechnung:

$$\begin{aligned}\left[11^1\right]_{35} &= 11\\ \left[11^2\right]_{35} &= 16\\ \left[11^4\right]_{35} &= 11\end{aligned}$$

Aufgabe 6.2. Erweiterter Euklidischer Algorithmus

a)

b)

c)

Aufgabe 6.3. Merkle-Hellmann-Verfahren

a)

b)

c)