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)

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

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 Nutze 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 und einfachem Zählen 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 wiederum 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)

$$\begin{aligned}
a &= 23 \\
b &= 17 \\
[a]_b &\overset{?}{\neq} 0 \quad \checkmark \\
r &= [23]_{17} = 6 \neq 0 \\
q &= \lfloor \frac{23}{17} \rfloor = 1 \\
(d, x, y) &= eEuklid(17, 6) \\
&= (1, -1, 3) \\
&\Rightarrow (d, y, x - qy) = (1, 3, -4)
\end{aligned}$$

b)

Wir zeigen zunächst Folgendes:

Theorem 1. *Falls* $a = \lfloor \frac{a}{b} \rfloor b + [a]_b = qb + r$*, dann ist* $ggt(a, b) = ggt(b, r)$

Beweis. Sei $d = ggT(a, b)$, also gilt

$$\begin{aligned}
a &= dn \\
b &= dm
\end{aligned}$$

Und daher

$$a - b = dn - dm = d(n - m) = dl$$

Also is d Teiler von a sowie von $a - b$. Alle gemeinsamen Teiler von a und b sind also Teiler von $a - b$. Deshalb gilt

$$b = a - (a - b) = dn - dl = d(n - l) = dk$$

und alle gemeinsamen Teiler von a und $a - b$ sind Teiler von b. Die wiederholte Subtraktion von b von a ändert also nichts an den gemeinsamen Teilern. Es folgt $ggT(a, b) = ggT(b, a) = ggT(b, a - b) = ggT(b, a - b - b) = \ldots = ggT(b, a - qb) = ggT(b, r)$. □

Es folgt also aus der zu zeigenden Aussage

$$\begin{aligned}
ggT(b, r) = xb + yr = ggT(a, b) &= ya + xb - qyb \\
yr &= ya - yqb \\
y[a]_b &= ya - yqb \\
&= ya - y\left\lfloor \frac{a}{b} \right\rfloor b \\
&= ya - y(a - [a]_b) \\
&= ya - ya + y[a]_b \\
&= y[a]_b
\end{aligned}$$

Da aus der Aussage eine Tautologie folgt, muss sie stimmen.

c)

Die Korrektheit ist nach **b)** trivial. Im zweiten Schritt berechnet der Algorithmus $(d, x, y) = eEuklid(b, r)$. Nach dem eben Gezeigten ist $d = d'$ mit $(d', x', y') = eEuklid(b, r)$. Im dritten Schritt gibt der Algorithmus neben dem ggT die beiden Faktoren y und $x - qy$ zurück. Nach Theorem 1 sind dies die richtigen Faktoren für $ggT(a, b)$.

Aufgabe 6.3. Merkle-Hellmann-Verfahren

a)

Um w^{-1} zu bestimmen, muss $eEuklid$ mit 385 und 17 durchgeführt werden. Das Ergebnis ist dann $(d, x, y) = (1, -3, 68)$. Wir überprüfen, ob es sich bei 68 tatsächlich um das multiplikativ Inverse von 17 in $\mathbb{Z}^*_{385}$ handelt.

$$[17 \cdot 68]_{385} = [1156]_{385} = 1$$

b)

Als öffentlichen Schlüssel haben wir gegeben $a = (17, 23, 46, 51, 92, 102, 184, 204)$ und $n = 385$.
Wir können so die Nachricht von Bob einfach verschlüsseln:

$$\begin{aligned} \mathit{Enc}_{a,n}(m) &= [< a, m >]_n \\ &= [< (17, 23, 46, 51, 92, 102, 184, 204), (1, 0, 1, 1, 1, 0, 1, 1) >]_{385} \\ &= [17 + 46 + 51 + 92 + 184 + 204]_{385} \\ &= [594]_{385} \\ &= 209 \end{aligned}$$

c)

Um die Nachricht zu entschlüsseln, müssen wir das folgende SubsetSum-Problem lösen:

$$\begin{aligned} \mathit{Dec}_{a,n}(c) &= \textsc{SubsetSum}\left(b, [c \cdot w^{-1}]_n\right) \\ &= \textsc{SubsetSum}\left(b, [17 \cdot 68]_{385}\right) \\ &= \textsc{SubsetSum}\left(b, [1156]_{385}\right) \\ &= \textsc{SubsetSum}\left(b, 208\right) \end{aligned}$$

Die fehlende Komponente b können wir berechnen:

$$\begin{aligned} b &= [w^{-1} \cdot a]_n \\ &= [68(17, 23, 46, 51, 92, 102, 184, 204)]_{385} \\ &= [(1156, 1564, 3128, 3468, 6256, 6936, 12512, 13872)]_{385} \\ &= (1, 24, 48, 3, 96, 6, 192, 12) \end{aligned}$$

Jetzt lösen wir das Problem:

$$\begin{aligned} \mathit{Dec}_{a,n}(c) &= \textsc{SubsetSum}\left((1, 24, 48, 3, 96, 6, 192, 12), 208\right) \\ &= (1, 0, 0, 1, 0, 0, 1, 1) \end{aligned}$$

Damit ist die Lösung $m = 10010011$.