Grundlagen Informations Sicherheit
Übungsblatt 04

Max Kurz (3265240) Mohamed Barbouchi (3233706)
Daniel Kurtz (3332911)

Problem 1

Sei $r_2 = (r_1 \mod N)^c$, dann gilt

$$\begin{aligned}
E^{r_1}(x, N)^c \mod N^2 &= ((1+N)^x \cdot r_1^N \mod N^2)^c \mod N^2 \\
&= ((1+N)^x \cdot r_1^N \mod N)^c \mod N^2 \\
&= ((1+N)^{x \cdot c} \cdot (r_1^N \mod N)^c) \mod N^2 \\
&= ((1+N)^{x \cdot c \mod N} \cdot (r_1^N \mod N)^c) \mod N^2
\end{aligned}$$

$$\begin{aligned}
E^{r_2}(cx \mod N, N) &= ((1+N)^{x \cdot c \mod N} \cdot r_2^N) \mod N^2 \\
&= ((1+N)^{x \cdot c \mod N} \cdot (r_1^N \mod N)^c \mod N^2
\end{aligned}$$

Wir sehen also dass $E^{r_1}(x, N)^c \mod N^2 = E^{r_2}(cx \mod N, N)$ gilt.

$\square$

Problem 2

1. $\phi(35) = (7-1)(5-1) = 6 \cdot 4 = 24$

2. Mit $\phi^{-1}(35) = 19$ berrechnen wir nun $D(1031, 24)$ und $D(776, 24)$

$$\begin{aligned} D(1031, 24) &= \left(\frac{(1031^{24} \mod 35^2) - 1}{35} \cdot 19\right) \mod 35 \\ &= \left(\frac{596 - 1}{35} \cdot 19\right) \mod 35 \\ &= (17 \cdot 19) \mod 35 \\ &= 24 \end{aligned}$$

$$\begin{aligned} D(776, 24) &= \left(\frac{(776^{24} \mod 35^2) - 1}{35} \cdot 19\right) \mod 35 \\ &= \left(\frac{1051 - 1}{35} \cdot 19\right) \mod 35 \\ &= (30 \cdot 19) \mod 35 \\ &= 10 \end{aligned}$$

   Wir erhalten somit $x_3 = 10 + 8 = 18$

3. $y_3 = (1031 \cdot 776) \mod N^2 = 131$ Berechne $D(131, 24)$

$$\begin{aligned} D(131, 24) &= \left(\frac{(131^{24} \mod 35^2) - 1}{35} \cdot 19\right) \mod 35 \\ &= \left(\frac{421 - 1}{35} \cdot 19\right) \mod 35 \\ &= (12 \cdot 19) \mod 35 \\ &= 18 \end{aligned}$$

   Es gilt also $x_3 == x_3'$

Problem 3

a) Nope. Man wähle $x_1 = 100$ und $x_2 = 010$ dann gilt $h(100) = h(010) = 2$

b) Nope. Für beliebigen Input x, lässt sich x_1 und x_2 vertauschen um eine Kollision zu erzeugen, da $x_1 \oplus x_2 = x_2 \oplus x_1$ gilt.

Problem 4

Sei $h'(x) = h'(y)$ dann gilt $x(0)h(x) = y(0)h(y)$
Da $|x(0)| = |y(0)|$ gilt, folgt somit dass $h(x) = h(y)$ gilt.

$\square$

Problem 5

Algorithm 1

Let x, and x' be random
`send`(x)
`receive`(t)
`send`(x')
`receive`(t')
$x'' = x \| (x'_1 \oplus t) \| x'_2 \| \ldots \| x'_{n-1}$
`return` x'', t