

Grundlagen Informations Sicherheit

Übungsblatt 04

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

Problem 1

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

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

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

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

□

Problem 2

1. $\phi(35) = (7 - 1)(5 - 1) = 6 \cdot 4 = 24$
2. Mit $\phi^{-1}(35) = 19$ berechnen wir nun $D(1031, 24)$ und $D(776, 24)$

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

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

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

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

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

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.

□

Problem 5

Algorithm 1

```
1: Let  $x$ , and  $x'$  be random
2: send( $x$ )
3: receive( $t$ )
4: send( $x'$ )
5: receive( $t'$ )
6:  $x'' = x \parallel (x'_1 \oplus t) \parallel x'_2 \parallel \dots \parallel x'_{n-1}$ 
7: return  $x'', t$ 
```
