Grundlagen Informations Sicherheit
Übungsblatt 04

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

Problem 1

$$\begin{aligned} f_1 \cdot_{\mathbb{F}_{2^8}} f_2 = f_1 \cdot_{\mathbb{Z}_2[x]} f_2 \mod g = \\ x^7 + x^5 + x^4 + x^2 + x \cdot_{\mathbb{Z}_2[x]} x^6 + x^4 + x + 1 \mod g = \\ x^{13} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + x \mod g = \end{aligned}$$

$= x^5 + x^4 + x^2 + x$

Problem 2

Seien f und p beliebige Polynome. Dann gilt:

$$\begin{aligned} \deg(f \cdot p) &= \deg(\sum a_i x^i \cdot \sum a_j x^i) \\ &= \deg(\max\{x^i\} \cdot \max\{x^j\}) \quad \forall a_i, a_j \neq 0 \\ &= \deg(x^i_{\max} \cdot x^j_{\max}) \\ &= \deg(\underbrace{(x_{\max} \cdot \ldots \cdot x_{\max})}_{\text{i-mal}} \cdot \underbrace{(x_{\max} \cdot \ldots \cdot x_{\max})}_{\text{j-mal}}) = \deg(\underbrace{x_{\max} \cdot \ldots \cdot x_{\max}}_{\text{i+j -mal}}) \\ &= \deg(x^{i+j}) \\ &= \deg(f) + \deg(g) \end{aligned}$$

□

Problem 3

Sei x und x' unterschiedlich aber es gilt $h_n(x) = h_n(x')$.

Algorithm 1

1: Generate Keypair $((n, e), (n, d))$
2: `send`(x)
3: `receive`(s) und $s =$ `PKCS-sig`$(x, (n, d)) = h_n(x)^d \mod n$
4: `output`(x', s)

Der Angreifer hat einen Vorteil von 1.
$V'(x', s, (n, e)) = V(h_n(x'), s, (n, e)) =$ `vaild`, da:

$$\begin{aligned} h_n(x') &= h_n(x) \text{ und} \\ s^e &= h_n(x)^{d^e} \mod n = h_n(x) \end{aligned}$$

Das bedeutet also dass der Angreifer ohne das Orakel mit dieser Message zubefragen, einen `valid`-Tag gefunden hat und somit immer das Game gewinnt.

Problem 4

Problem 5