Crypto 2 Zusatzübung

Ex 4.) a.) - easy to compute

- preimage resistant
- second preimage resistant
- collision free

b.) $h: \mathbb{N} \mapsto A$

$\Rightarrow f: \mathbb{R} \mapsto [0,1)$ da $f(x) = x - \lfloor x \rfloor$,

$\lfloor x \rfloor = \max \{k \in \mathbb{Z} \mid k \leq x\}$

$h(n) - d \in \{0, 1, \dots, c-1\}$

$\Rightarrow h(n) \in \{d, d+1, \dots, d+c-1\} = A$

c.) $(c,d) = (99, 1)$ Find a collision

$h(1) = 42$, $h(100) = 42$

d.) $A \stackrel{!}{=} \{1, \dots, p-1\} \Rightarrow d = 1$, $c = 3732$

as hash parameters

e.) ElGamal Sig. $(p, \alpha, y) = (3733, 2, 1061)$

$h(m_1) = 2738$, $h(m_2) = 1537$

$(r_1, s_1) = (557, 3153)$, $(r_2, s_2) = (557, 1504)$

Alice has chosen the same session key twice!

f.) $s_1 = k_1^{-1}(h(m_1) - x \cdot r_1) \mod (p-1)$

$s_2 = k_2\ (h(m_2) - x \cdot r_2) \mod (p-1)$

$k = k_1 = k_2 \qquad r_1 = a^{k_1} \mod p = r_2 = r$

$\Rightarrow (s_1 - s_2) = k^{-1}(h(m_1) - h(m_2)) \pmod{p-1}$

$\Leftrightarrow k \equiv (h(m_1) - h(m_2))(s_1 - s_2)^{-1} \pmod{p-1}$

$h(m_1) - h(m_2) = 60 \qquad s_1 - s_2 = 1649$

$\gcd(3732, 1649) = 1$

$= 19 \cdot 3732 - 43 \cdot 1649$

$(s_1 - s_2)^{-1} = -43 \mod 3732$

$k = 607 \cdot (-43) = 23 \mod 3732$

$s_1 \equiv k_1^{-1}(h(m_1) - x \cdot r_1) \Leftrightarrow x \equiv r^{-1}(h(m_1) - k \cdot s_1)$

$\gcd(3732, 557) = 1 = 10 \cdot 3732 - 67 \cdot 557$

$\Rightarrow x = -67 \cdot (2138 - 23 \cdot 3153) \equiv 2011 \mod 3732$

$\Rightarrow k = k_1 = k_2 \wedge x = 2011$

Ex 5.)

a.) Euler's criterion: $p > 2$ prime:

$c \in \mathbb{Z}_p^* \text{ is QR iff } c^{\frac{p-1}{2}} \equiv 1 \mod p$

b.)

$p = 4k - 1, \quad k \in \mathbb{N}, \quad p > 2$

$\Leftrightarrow k = \frac{p+1}{4}$

show that $x_{1/2} \equiv \pm c^k \mod p$ solves $x^2 \equiv c \mod p$

$\Rightarrow (x_{1/2})^2 \equiv ((\pm c)^2)^{\frac{p+1}{4}}$

Crypto 2 Zusatzübung

$$\equiv c^{\frac{p+1}{2}} \equiv c \cdot \underbrace{c^{\frac{p-1}{2}}}_{\equiv 1 \text{ nach a.)}} \equiv c \mod p$$

c.)

$p = 47,\ q = 79$, i.e., $p = 4 \cdot \underset{\substack{\Downarrow \\ k}}{12} - 1$, $q = 4 \cdot \underset{\substack{\Downarrow \\ k}}{20} - 1$

with b.)

$$7^{12} = (7^2)^6 \equiv 2^6 \equiv 64 \equiv 17 \mod 47$$

$$\Rightarrow \underset{\substack{\uparrow \\ c}}{17}^2 \equiv 7 \mod 47 \wedge \underset{\substack{\uparrow \\ -c}}{30}^2 \equiv 7 \mod 47$$

with b.)

$$5^{20} \equiv 25^{10} \equiv (\underbrace{25^2}_{\equiv -7})^5 \equiv (-7)^5 \equiv 20 \mod 79$$

$$\Rightarrow \underset{\substack{\uparrow \\ c}}{20}^2 \equiv 5 \mod 79 \wedge \underset{\substack{\uparrow \\ -c}}{59}^2 \equiv 5 \mod 79$$

d.)

$n = p \cdot q = 47 \cdot 79 = 3713$

It is $p, q \equiv 3 \mod 4$

To calculate: $x^2 \equiv 242 \mod 47 \equiv 7$

$y^2 \equiv 242 \mod 79 \equiv 5$

Hint: $sp + tq = 37 \cdot 47 - 22 \cdot 79 = 1$

$s = 37,\ p = 47,\ t = -22\ \ q = 79$

$a = -1738,\ b = 1739$

$$(\mathrm{mod}\ n)\quad \begin{aligned} f_1 &= ax + by \equiv -1738 \cdot 17 + 1739 \cdot \mathbf{20} \equiv -29546 + 34760 \\ &\equiv 1521 = (\ldots 001)_2 \\ f_2 &= ax - by \equiv 158 - 1363 \equiv 2508 \equiv (\ldots 100)_2 \\ f_3 &= -ax + by \equiv -158 + 1363 \equiv 12005 \equiv (\ldots 101)_2 \\ f_4 &= -ax - by \equiv -158 - 1363 \equiv 2192 \equiv (\ldots 000)_2 \end{aligned}$$

Ex 6.)

a.) General: $E: y^2 = x^3 + a \cdot x + b$

Here: $E: y^2 = x^3 + b$ over $\mathbb{F}_5$

$\Rightarrow a = 0,$

Discriminant $\Delta = (-16) \cdot (4a^3 + 27b^2) \overset{!}{\not\equiv} 0 \mod 5$

$\Leftrightarrow \Delta \equiv 4\,(2b^2) \equiv 3b^2 \overset{!}{\not\equiv} 0 \mod 5$

$\Rightarrow b \in \{1, 2, 3, 4\} = \mathbb{Z}_5^*$

b.) $(3,1): \; 1^2 = 3^3 + b \Leftrightarrow b \equiv 4 \mod 5$

$(4,4): \; 4^2 = 4^3 + b \Leftrightarrow b \equiv 2 \mod 5$

There is no b, ...

c.) $b = 3 \qquad E: y^2 = x^3 + 3$

z	z^2	z^3	$z^3 + 3$
0	0	0	3
1	1	1	4
2	4	3	1
3	4	2	0
4	1	4	**2**

(mod 5)

$z^2 \in \{0, 1, 4,\} = A$

$z^3 + 3 \in \{0, 1, 2, 3, 4\} = B$

Crypto 2 Zusatzübung

24. FEB. 2012

Candidates for $A \cap B = A$

$$\left.\begin{array}{l} z^3+3=0 \iff z = x = 3 \\ z^2 = 0 \iff z = y = 0 \end{array}\right\} \Rightarrow (3,0) \in E(\mathbb{F}_5)$$

$z^3+3 = 1 = z^2 \iff x = 2 \wedge y \in \{1,4\} \Rightarrow (2,1),(2,4) \in E(\mathbb{F}_5)$

$z^3+3 = 4 = z^2 \iff x = 1 \wedge y \in \{2,3\} \Rightarrow (1,2),(1,3) \in E(\mathbb{F}_5)$

$E(\mathbb{F}_5) = \{(3,0),(2,1),(2,4),(1,2)(1,3),\mathcal{O}\}$

c.) $\# E(\mathbb{F}_6) = 6 = q+1-t \Rightarrow t = \overset{\text{old } p \text{ value}}{q}+1-\# E(\mathbb{F}_5)$

$= 5+1-6 = 0$

$\Rightarrow \underline{\underline{t=0}}$

d.)

$-(3,0) = (3,0)$

$-(2,1) = (2,4)$

$-(2,4) = (2,1)$

$-(1,2) = (1,3)$

$-(1,3) = (1,2)$

$-\mathcal{O} = \mathcal{O}$

e.) $(1,2)$

bis hier berechnen

$0 \cdot (1,2) = \mathcal{O}$

$1 \cdot (1,2) = (1,2)$

$2 \cdot (1,2) = (2,1)$

- evtl. Inversen in Tabelle dazu berechnen

ab hier kombinieren

$3 \cdot (1,2) = 2(1,2)+(1,2)$
$= (3,0)$

- Formel anwenden

$4 \cdot (1,2) = 3(1,2)+(1,2) = (2,4)$

$5 \cdot (1,2) = 4(1,2)+(1,2) = (1,3)$, $6 \cdot (1,2) = \mathcal{O}$ }

f.) $\mathcal{O} = 2P \Rightarrow (3,0) \vee P = \mathcal{O}$

$= 2 \cdot (3,0) = 2 \cdot 3 \cdot (1,2) = 6 \cdot (1,2) = \mathcal{O}$

g.) $Q = a \cdot P \qquad P \in E(\mathbb{F}_q),\ a \in \mathbb{Z}$

$Q \in \langle P \rangle$

a is the discrete logarithm to base P.
Problem to find a.