Crypto 2 Ü 8

Ex 23.) El-Gamal-Signature-Scheme

Parameters: 1.) p prime

2.) a generator (primitive element) mod p

3.) $x \in \{2, \dots, p-2\}$ private key

4.) Alg. 11 $\gcd(k, p-1) = 1$

a.) i.) 4793 is prime

ii.) Prop 7.5. $p - 1 = \prod_{i=1}^{l} p_i^{t_i}$ prime factorization, p prime

a is PE mod p

$\Leftrightarrow a^{\frac{(p-1)}{p_i}} \not\equiv 1 \pmod{p} \quad \forall i = 1, \dots, l$

$p = 4793 \Rightarrow p-1 = 4792 = 2^3 \cdot 599 = p_1^{t_1} \cdot p_2$

$a = 4792 \equiv -1 \mod 4793$

$\Rightarrow a^{4792/599} = a^8 \equiv 1 \pmod{4793}$ ϟ

$a = 1400$: $p_1 = 2 \quad 1400^{4792/2} \overset{SQM}{\equiv} 4792 \not\equiv 1 \pmod{4793}$

$p_2 = 599 \quad 1400^8 \equiv 2691 \not\equiv 1 \pmod{4793}$

$\Rightarrow a = 1400$ is PE

iii.) $x = 9177 \quad 9177 > p-2$ ϟ

$x = 257 \quad 2 \leq 257 \leq p-2$ ✓

iv.) $\gcd(2811, 4792) = 1$ ✓

b.)

Sign message $m = 231$ using $p = 4793$, $x = 257$, $a = 1400$, $k = 2811$

Follow Alg. 11

- „$r \leftarrow a^k \bmod p$": $r = 1400^{2811} \bmod 4793 \overset{SQM}{=} 2666$
- „computing $k^{-1} \bmod p-1$": possible as $\gcd(k, p-1) = 1$

Extended Euclidean Algorithm: $-1045 \cdot 2811 + 613 \cdot 4792 = 1$

$\Rightarrow k^{-1} \equiv -1045 \equiv 3747 \pmod{4792}$

- „$s \leftarrow k^{-1}(m - x \cdot r) \bmod (p-1)$":

$3747(231 - 257 \cdot 2666) \bmod 4792 = 607$

$\Rightarrow \langle r, s \rangle = \langle 2666, 607 \rangle$

Ex 24.)

El Gamal signature scheme

$m = 65$, $y = 399$, $p = 859$, $a = 206$, $\langle r, s \rangle = \langle 373, 15 \rangle$

Verification: Algorithm 12

1.) „$1 \le r \le p-1$": $1 \le 373 \le 858$ ✓

2.) „$v_1 \leftarrow y^r \cdot r^s \bmod p$":

$v_1 = 399^{373} \cdot 373^{15} \equiv 672 \cdot 643 \equiv 19 \pmod{p = 859}$

3.) „$v_2 \leftarrow a^m \bmod p$":

$v_2 = 206^{65} \bmod 859 = 19$

4.) „$v_1 = v_2$?": Yes: signature is valid

Ex 25.)

In the El Gamal verification scheme (Alg. 12, Ex 24.) verify $v_1 \equiv v_2 \pmod p$ needs to be fulfilled

$$\Leftrightarrow y^r \cdot r^s \equiv a^{h(m)} \pmod p$$

$$y = a^x \bmod p$$

$$r = a^k \bmod p \quad \text{(Alg. 11)}$$

$$\Leftrightarrow a^{x \cdot r} a^{k \cdot s} \equiv a^{h(m)} \pmod p$$

Fermat

$$\Leftrightarrow x \cdot r + k \cdot s \equiv h(m) \pmod{(p-1)}$$

$h(m)^{-1}$ ex.

$$\Leftrightarrow x \cdot \underbrace{r \cdot h(m)^{-1} \cdot h(m')}_{r'} + k \cdot \underbrace{s \cdot h(m)^{-1} \cdot h(m')}_{s'} \equiv \overbrace{h(m) \cdot h(m)^{-1} \cdot h(m')}^{h(m')} \bmod p-1 \quad (*)$$

$$\Leftrightarrow x \cdot r' + k \cdot s' = h(m') \pmod{p-1}$$

Fermat

$$\Leftrightarrow a^{x \cdot r'} + a^{k \cdot s'} \equiv a^{h(m')} \bmod p$$

$$\Leftrightarrow y^{r'} \cdot r^{s'} \equiv a^{h(m')} \pmod p$$

$$\overset{!}{\Leftrightarrow} y^{r'} \cdot r'^{s'} \equiv a^{h(m')} \pmod p$$

equivalence assumption holds, if $r \equiv r' \bmod p$ and from $(*)$

$$r \cdot h(m)^{-1} h(m') \equiv r' \pmod{p-1}$$

By means of chinese remainder theorem 6.10 we get:

$a_1 = r \bmod p \qquad a_2 = r\, h(m)^{-1} h(m') \bmod p-1$

$m_1 = p \,, \quad m_2 = p-1 \,, \quad M_1 = p-1 \,, \quad M_2 = p \,, \quad M = p(p-1)$

$y_1 = M_1^{-1} \bmod p = p-1 \,,$

$y_2 = M_2^{-1} \bmod p-1 = 1$

$$\Rightarrow x = r' = \sum_{i=1}^{2} a_i M_i y_i = r \cdot (p-1)^2 + r\, h(m)^{-1} h(m') \cdot p \mod M (= p(p-1))$$

$$\equiv r (\underbrace{p^2 - p}_{p(p-1)} - p + 1 + h(m)^{-1} h(m') \cdot p)$$

$$\equiv r (h(m)^{-1} h(m') \cdot p - p + 1)$$

$\langle r', s' \rangle = \langle r(h(m)^{-1} h(m') \cdot p - p + 1), s \cdot h(m)^{-1} h(m') \rangle$

is a valid signature of $h(m')$, iff

$1 \leq r \leq p$ is <u>not</u> checked.