Crypto 2 Ü9 20. DEZ. 2011

Ex 26.) ElGamal verification

a.) Let $s \equiv x^{-1}(h(m) - k \cdot r) \pmod{p-1}$ //signature

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

Parameters of ElGamal

$r \equiv a^k \mod p$, a is a PE mod p

$y \equiv a^x \mod p$

$$y^s \cdot r^r \equiv a^{x \cdot s} \cdot a^{k \cdot r} \equiv a^{sx+kr} \underset{\uparrow}{\equiv} a^{h(m) \cancel{- k \cdot r + k \cdot r}}$$

$sx \equiv h(m) - kr \pmod{p-1}$

$$\equiv a^{h(m)}$$

$\square$

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

$$a^? \equiv y^? \cdot r^? \Rightarrow a^s \equiv a^{x \cdot h(m)} \cdot a^{k \cdot r}$$
$$\equiv y^{h(m)} \cdot r^r$$

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

$$\Rightarrow a^s \equiv a^{x \cdot r} \cdot a^{k \cdot h(m)} \equiv a^s \equiv y^r \cdot r^{h(m)}$$

Ex 27.) DSA - Signing and verification

Sign $h(m)$ 18723 with a DSA signature
$p = 27583$; $q = 4597$, $a = 504$, $y = 23374$
$x = 1860$, $k = 1773$

DSA signing

1.) $k \in \{2, \ldots, q-2\}$ ✓

2.) $r = (a^k \bmod p) \bmod q \equiv (14463) \bmod 4597$ // sqm
$\equiv 672 \bmod 4597$

3.) $k^{-1} \bmod q$: $k \cdot k^{-1} + q \cdot q^{-1} = 1$
$\Rightarrow \underbrace{503}_{k^{-1}} \cdot \underbrace{1773}_{k} - \underbrace{194}_{q^{-1}} \cdot \underbrace{4597}_{q} = 1$

4.) $s = k^{-1}(h(m) + x \cdot r) \bmod q$
$= 503 \cdot (18723 + 1860 \cdot 672) \bmod 4597$
$= 4068 \bmod 4597$

5.) $(r, s) = (672, 4068)$

DSA verification

1.) $0 < r = 672 < q = 4597$ ✓
$0 < s = 4068 < q = 4597$ ✓

2.) $w = s^{-1} \bmod q$: $s \cdot s^{-1} + q \cdot q^{-1} = 1$ // Ext. EA
$\underbrace{-869}_{s^{-1}} \cdot \underbrace{4068}_{s} + \underbrace{769}_{q^{-1}} \cdot \underbrace{4597}_{q} = 1$

$s^{-1} \bmod q \equiv -869 \equiv 3728 \bmod 4597$

3.) $u_1 \equiv w \cdot h(m) \mod q = 3728 \cdot 18723$
$\equiv 3093 \mod 4597$

$u_2 \equiv r \cdot w \mod q = 672 \cdot 3728 \equiv 4448 \mod 4597$

4.) $v = (a^{u_1} \cdot y^{u_2} \mod p) \mod q = ((504^{3093} \cdot 23374^{4448})$
$(\mod 27583)) \mod 4597$

$\equiv \underbrace{8228 \cdot 25275}$

$\equiv 14463 \mod 27583 \mod 4597$

$\equiv \underline{\underline{672}} \mod 4597$

✓

Ex 28.) DSA - Finding a cyclic subgroup of order q

Given: $g \in \mathbb{Z}_p^*$, $a \equiv g^{\frac{p-1}{q}} \mod p$,
$q \mid (p-1)$, primes p, q, $a \neq 1$

By definition of the order of a group
$ord(a) = \min \{ k \in \{1, \ldots, \varphi(p)\} \mid a^k \equiv 1 \mod p \} \}$
(Def 7.1)

$\Rightarrow a^{ord(p(a))} \equiv 1 \mod p$

with $a \neq 1 \Rightarrow ord(p(a)) > 1$

$a^q \equiv (g^{(p-1)/q})^q \equiv g^{p-1} \equiv 1$
↑ Fermat's Th. $g \in \mathbb{Z}_p^*$

$1 < \text{ord}(p(a)) \leq q$

- Does $k < q$ exist? (Proof by contradiction)
- Assume the ~~...~~ subgroup has $k = \text{ord}(p(a)) < q$

Then $\Rightarrow a^q \equiv a^{lk+r} \bmod p \quad l \in \mathbb{Z},\ r<k$

$\equiv a^r \bmod p \equiv 1 \bmod p$

1.) $\text{ord}(p(a)) \nmid q \Rightarrow a^r \equiv 1 \bmod p$ with $1<r<\text{ord}(p(a))$

2.) $\text{ord}(p(a)) \mid q \Rightarrow a^0 \equiv 1 \bmod p$ ✓

q is prime $\Rightarrow \text{ord}(p(a)) \mid q$ only if $\text{ord}(p(a)) = 1$

$a \neq 1$

or $\text{ord}(p(a)) \equiv q$ ✓

$\Rightarrow$ The cyclic subgroup has order q in $\mathbb{Z}_p^*$ if a is chosen according to the given algorithm. $\square$