Digital Signatures

Tutorial

Q: one-time secret k repeated.

what will happen.

$(s_2, s_1) - m$

$(s_2', s_1') - m'$ } k

$$m = s_2 k + x_A s_1$$

$$m' = s_2' k + x_A s_1'$$

k, x_A

$s_1 = g^k$

$s_1' = g^k$

$$m - m' = k(s_2 - s_2') + \underline{x_A (s_1 - s_1')}$$

$$\Rightarrow m - m' = k(s_2 - s_2')$$

$$\Rightarrow \boxed{k = \frac{m - m'}{s_2 - s_2'}}$$

$\boxed{g, g^k \Rightarrow k}$

solving DLP.

Q: Z_p, g - generator
p - large prime

choose $x \in Z_p^*$

public key $\underline{y = g^x} \in Z_p$

Declare (g, y, p)

ElGamal type Signature

Signature Algorithm: (r, s) signature on m.

$$m = H(m)$$

$\underline{r} = g^k \bmod p$, where k, $(k, \phi(p)) = 1$.

$$s = [k^{-1}x - k^{-1}r - k^{-1}m] \pmod{\phi(p)}$$

Q1: Design the signature Verification Algorithm

$$\boxed{\begin{matrix} m, \ (r, s) \\ (g, y, p) \end{matrix}}$$ known

$$s = k^{-1}(x - r - m)$$

$$ks = x - r - m$$

$$ks = x - (r + m)$$

$$\boxed{x = ks + (r+m)}$$

$$g^x = g^{ks + (r+m)}$$

$$\boxed{y = r^s \cdot g^{(r+m)}}$$

Verification algorithm

Q) finite field $\mathbb{Z}_{101}$ with base-point $g = 12$

→ selects $x = 28$

random $K = 13$

$H(m) = m = 21$ (assume).

⇒ find the signature with detailed steps?

⇒ also verification in detail?

$y = g^x = 12^{28} \pmod{101} = \underline{\underline{92}}$

$r = g^k \pmod{101}$, $(K, \phi(p)) = 1$

$(13, 100) = 1$.

$s = K^{-1}(x - r - m) \bmod \phi(p)$.

$r = 12^{13} \pmod{101} = 53$

$K^{-1} = 13^{-1} \equiv 77 \pmod{100}$

$s = 77(28 - 53 - 21) \pmod{100}$

$= 58$

Signature on m is

$(r, s) = (53, 58)$.

Verification: $r^s \cdot g^{r+m} = 53^{58} * 12^{53+21} \pmod{101}$

$= 92$

$= \underline{\underline{y}}$