Semester: VI Subject: CSS Academic Year: 2023-2024

ELGAMAL DIGITAL SIGNATURE SCHEME:

* The ElGamal digital signature scheme stems from the ElGamal cryptosystem based upon the security of the one-way function of exponentiation
* The ElGamal signature scheme involves the use of the private key of sender for encryption and the public key of sender for decryption. The algorithm creates two different signatures, these 2 signatures are used in the verification phase.

Key Generation:

* The key generation process is same as that of El-Gamal cryptosystem.
* Sender chooses prime no. p and primitive root e_1.
* Then he computes $\boxed{e_2 = e_1^d \bmod p}$
* Sender publishes public key = (e_1, e_2, p) and retains the private key = d.

Working:

Step 1: Signing. [The sender signs]

* The sender selects the random number r.
* The sender computes the first signature

$$\boxed{S_1 = e_1^r \bmod p}$$

* The sender computes the second signature S_2 using the equation: $\boxed{S_2 = (M - d * S_1) * r^{-1} \bmod (p-1)}$

where:

P = large prime numbers.

M = original message that needs to be signed.

* The sender sends M, S_1 and S_2 to the receiver.

Step 2: Verifying.

The receiver receives M, S_1 and S_2 which can be verified as follows:

* The receiver checks to see if $0 < S_1 < p$.
* The receiver checks to see if $0 < S_2 < p-1$.
* The receiver performs first part of verification, V_1 using the equation:

$$\boxed{V_1 = e_1^{M} \bmod p}.$$

* The receiver performs second part of verification, V_2 using the equation:

$$\boxed{V_2 = e_2^{S_1} * (S_1^{(S_2)} \bmod p}$$

* If $V_1 \equiv V_2$, the signature is valid and the message is accepted, Otherwise, it is rejected.

Example:

Key Generation:-

prime number $p = 19$.

Select e_1 = primitive root of p

$$\begin{array}{r|l} 2 & 18 \\ 3 & 9 \\ & 3. \end{array}$$

$p = 19$

$\phi(p) = (p-1) = (19-1) = 18$

$18 = 2 \times 3^2$.

Calculate $n_i = \phi(p)/p_i$.

$18/2 = 9$.

$18/3 = 6$.

$\left.\begin{array}{l} 2^9 \bmod 18 = 8 \\ 2^6 \bmod 18 = 10 \end{array}\right\}$ 2 is primitive root.

$\left.\begin{array}{l} 10^9 \bmod 18 = 10 \\ 10^6 \bmod 18 = 10 \end{array}\right\}$ This is also primitive root.

$\boxed{e_1 = 10}$

In this case we choose 10.

Gcd $(10, 19) = 1$

Select d $1 < d \leq p-2$

$\boxed{d = 16}$ $\rightarrow$ private key.

Compute e_2:

$\boxed{e_2 = e_1^d \bmod p}$

$= (10)^{16} \bmod 19$.

$\boxed{e_2 = 4}$

Publickey $\boxed{= (e_1, e_2, p) = (10, 4, 19)}$

The user publisheds his public key.

Sender has to generate the Signature:
(X)

Sender X wants to send $M = 4$ to Y.

Note: Message $M < p$.

$m = H(M) = H(4) = 14$ [Assume that hash function of (value) 4 is 14]

The sender selects the random number ($r=5$).
Such that $\gcd(r, p-1) = 1$.
$\gcd(5, 18) = 1$.

Compute S_1 & S_2:-

$$\boxed{S_1 = e_1^r \bmod p}$$

$$= 10^5 \bmod 19.$$

$$\boxed{S_1 = 3}$$

$$S_2 = (M - dS_1)\, r^{-1} \bmod (p-1).$$

$r^{-1} \bmod (p-1)$.

$5^{-1} \bmod 18 \implies 5 * 11 \bmod 18 = 1.$

$$S_2 = 11(14 - (16)(3)) \bmod 18.$$

$$= 11(-34) \bmod 18.$$

$$= -374 \bmod 18.$$

$$\boxed{S_2 = 4}$$

The signature of X is (S_1, S_2). The message $\boxed{M=4}$ is send with signature $\boxed{S_1 = 3,\ S_2 = 4}$ to Y.

The Receiver Y receives $M=4$
$S_1=3$
$S_2=4$.

The Receiver Y should verify the signature. So that he will know that the message is not modified and received from right sender.

Semester: VI Subject: CSS Academic Year: 2023-2024

Verifying: (Receiver Y)

$$\boxed{V_1 = e_1^{M} \bmod p}$$

$$V_1 = (10)^{14} \bmod 19$$

$$\boxed{V_1 = 16}$$

$$V_2 = (e_2^{S_1})(S_1)^{S_2} \bmod p.$$

$$= (4)^3 (3)^4 \bmod 19.$$

$$= 5184 \bmod 19.$$

$$\boxed{V_2 = 16.}$$

The signature is valid if $V1 \equiv V_2$.