* Digital Signatures :-

→ This belongs to asymmetric key cryptography

encryption - private key

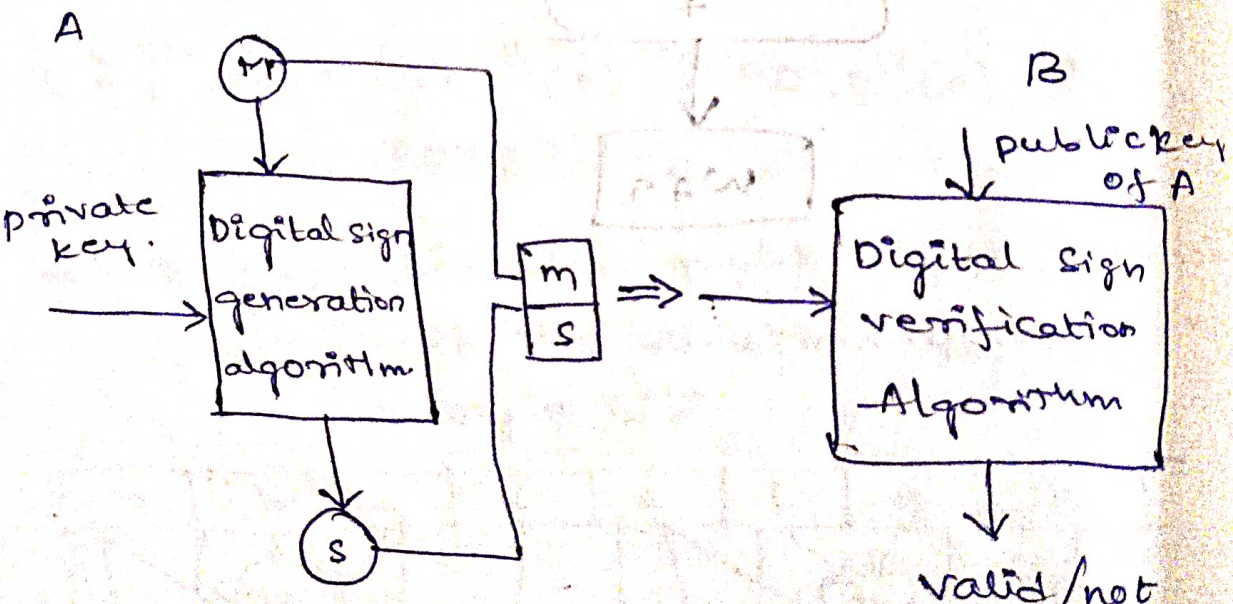
decryption - public key.

→ used for both authentication (msg is being sent to correct person or not) and Non-Repudiation (msg can't be denied)

→ Signature - proof of identity

(checks whether the msg is from correct sender or not)

→ working :-



if msg matches ⇒ valid

if msg not matching ⇒ invalid.

3 steps :-

1) Key generation - public & private keys generation

2) Signing process - use private key to sign a message. This private key along with public key, creates digital signature

3) Verification - using public key.

* Elgamal digital Signature scheme:-

→ Encryption - public key
decryption - private key.

→ working :-

1. select a prime number(q)
2. select a primitive root(α) of q
3. Generate a random integer (x_A)
$1 < x_A < q-1$
4. compute $Y_A = (\alpha)^{x_A} \bmod q$
5. Generate keys for user A
private key $\Rightarrow x_A$
public key $\Rightarrow \{q, \alpha, Y_A\}$

$\alpha^n \bmod q$
$n \in [0, q-2]$
all are distinct values

key generation

6. Generate hashcode (m) for plaintext (M)
$m = H(M)$ $0 \le m \le q-1$
7. Generate a random integer k
$1 \le k \le q-1$ and $\gcd(k, q-1) = 1$
8. Now calculate s_1 and s_2,
$s_1 = \alpha^k \bmod q$
$s_2 = k^{-1}(m - x_A s_1) \bmod q-1$

signing process.

9. Now we got signature pair (s_1, s_2)

Now at user B's side,

Calculate v_1 & v_2

$v_1 = \alpha^m \bmod q$

$v_2 = (Y_A)^{s_1} \cdot (s_1)^{s_2} \bmod q$

verification

if $v_1 = v_2 \Rightarrow$ Signature is valid

else $\Rightarrow$ Signature is not valid.

Ex:- let $q = 19$ and $\alpha = 10$

Now random integer x_A $(1 < x_A < q-1)$

$$1 < x_A < 18$$

$$\boxed{x_A = 16}$$

$$Y_A = \alpha^{x_A} \bmod q = (10)^{16} \bmod 19$$

$$= 4$$

$$\boxed{Y_A = 4}$$

$\therefore$ A $\Rightarrow$ private key = 16

public key = $\{19, 10, 4\}$

Now, generate hash code(m)

$$m = H(M) \quad 0 \le m \le q-1$$

$$0 \le m \le 18$$

$$\boxed{m = 14}$$

Generate a random integer k

$$0 \le k \le q-1 \text{ and } \gcd(k, q-1) = 1$$

$$0 \le k \le 18 \text{ and } \gcd(k, 18) = 1$$

$$\boxed{k = 5}$$

Calculate $s_1 = \alpha^k \bmod q$

$$= (10)^5 \bmod 19$$

$$= 3$$

$$\boxed{s_1 = 3}$$

$$s_2 = k^{-1}(m - x_A s_1) \bmod q-1$$

$k^{-1} \Rightarrow k^{-1} \bmod q-1$

$\Rightarrow 5^{-1} \bmod 18.$

$\Rightarrow 5x \stackrel{?}{=} 1 \pmod{18}$ $\quad \frac{5 \times 11}{18} = 1$

$$\boxed{k^{-1} = 11}$$

$S_2 = k^{-1}(m - x_A S_1) \bmod q-1$

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

$= -374 \bmod 18 = 4$

$(S_1, S_2) = (3, 4)$

B => $V_1 = \alpha^m \bmod q$

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

$= 16$

$\boxed{V_1 = 16}$

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$

$= 4^3 \times 3^4 \bmod 19$

$= 5184 \bmod 19$

$\boxed{V_2 = 16}$

$V_1 = V_2$ => Signature is valid.

* Schnorr digital signature scheme :-

→ Simple and efficient as well as faster.

→ working :-

1. Select a prime number (q)
2. Select a primitive root (α) of q
3. Generate a random integer x_A

$1 < x_A < q-1$

4. Compute $Y_A = (\alpha)^{x_A} \bmod q$
5. Generate keys for sender

private key = x_A

public key = $\{q, \alpha, Y_A\}$

6, Generate a random integer k

$$1 < k < q-1$$

7, compute $R = (\alpha)^k \bmod q$

8, Concaterat R & plain text and then compute hash value.

$$e = H(R \| M)$$

9, Compute $s = k + x_A \cdot e \bmod (q-1)$

10, signature pair = (R, s)

At B's end :-

$$e' = H(R \| M)$$

$$S = (\alpha)^s \cdot y_A^{-e'} \bmod q$$

$$R' = (\alpha)^S \cdot R \bmod q$$

if $R' \equiv R \bmod p$ — signature is valid

else — signature is not valid.

Ex:- $q = 101 \quad \alpha = 2$

$x_A = 7$ $\quad 1 < x_A < 101-1$

$Y_A = (\alpha)^{x_A} \bmod q$

$= (2)^7 \bmod 101 \quad = 128 \bmod 101$

$Y_A = 72$

A ⇒ private key = 7

public key = {101, 2, 72}

$k = 13$ $\quad 1 < k < 100$

$R = (\alpha)^k \bmod q$

$= 2^{13} \bmod 101$

$\boxed{R = 95}$

$e = H(95 \| m)$

$= |37|$ assume

$\boxed{e = 37}$

$s = (13 + 7 \cdot 37) \bmod 100$

$= 314 \bmod 100$

$\boxed{s = 14}$

Signature pair = $(R, s) = (95, 14)$

B ⇒

$e' = H(R \| M) = 37$

$S = (\alpha)^s \cdot y_A^{-e'} \bmod q$

$= (2)^{14} \cdot (72)^{-37} \bmod 101 = 28$

$R' = (\alpha)^s \cdot R \bmod q$

$= (2)^{28} \cdot 95 \bmod 101$

$= 95$

$R' \equiv R \bmod 101$

$\equiv 95 \bmod 101$

$= 95$

∴ signature is valid.