UNIT - 2

① RSA algorithm Prerquisites

ⓐ Modulus Arithmatic

$36 \equiv 24 \bmod 12$

i) If $x \equiv y \bmod n$ & $a \equiv b \bmod n$
then $(x+a) \equiv (y+b) \bmod n$
and $(x-a) \equiv (y-b) \bmod n$
and $(x \times a) \equiv (y \times b) \bmod n$

ii) If & $x \equiv (y \times z) \bmod n$,
then $x \equiv (y \bmod n \times z \bmod n) \bmod n$

iii) If $x \equiv (y+z) \bmod n$,
then $x \equiv (y \bmod n + z \bmod n) \bmod n$

ⓑ Eular's Totient Function

$\phi(n)$ for $[n \geq 1]$ is defined as as the no. of +ve integers $< n$, that are co prime of n.

$\phi(6) = \{1, 5\} = (2)$

* only for primes,
$\phi(n) = n-1$
$\phi(a*b) = \phi(a) * \phi(b)$ [if $\gcd(a, b) = 1$]

(c) Multiplicative Inverse

If $x \not\equiv 0 \bmod n$ (if n is prime)
and $x \cdot y \equiv 1 \bmod n$,
then y is multiplicative inverse of $x \bmod n$

If n is not prime,
x & n should be coprime [$\gcd(x, n) = 1$]

(d) Eular's theorem

If x & n are coprime [$\gcd(x, n) = 1$],
then $x^{\Phi(n)} \equiv 1 \bmod n$

(e) Fermet's theorem (IMP)

$x^{n-1} \equiv 1 \bmod n$ when n = prime
x not divisible by n

$x^n \equiv x \bmod n$ (when $\gcd(x, n) = 1$)

② RSA algorithm

a) Choose 2 prime numbers p & q.
Let $p = 61$, $q = 53$

b) Compute $n = p \times q = 3233$

c) $\phi(n) = \phi(p) \times \phi(q) = 60 \times 52 = 3120$

d) Choose 'e' such that $1 \leq e \leq \phi(n)$, coprime to $\phi(n)$.

→ ~~Pbl~~ Public key = $(e, n) = (17, 3233)$

e) Determine 'd' as $ed = 1 \bmod \phi(n)$
$d = e^{-1} \bmod \phi(n)$

$$\Rightarrow d = \frac{(\phi(n) \times i) + 1}{e}$$

→ Private key = $(d, n) = (2753, 3233)$

③ Encryption & Decryption with RSA

Encryption	Decryption
$C = P^e \bmod n$	$P = C^d \bmod n$

④ Attacks on RSA algorithm

a) Brute force : Try all private keys

b) Mathematical attacks : Factoring product of 2 primes.

c) Timing attack : running time of decryption algo.

d) Chosen cypher attacks

(5) Diffie - Hellman Key exchange

→ Used to exchange secret keys.

Steps :-

i) Consider a prime no. q.

ii) Select α such that it is a primitive root of q and $\alpha < q$.

→ α & q are public

iii) User A's private key $X_A < q$

iv) Calculate A's public key $Y_A = \alpha^{X_A} \bmod q$

v) User B's private key $X_B < q$.

vi) Calculate B's public key $Y_B = \alpha^{X_B} \bmod q$

vii) Calculate secret key by A :

$$K = Y_B^{X_A} \bmod q$$

viii) Calculate secret key by B :

$$K = Y_A^{X_B} \bmod q$$

Example : $q = 7$

$\alpha = 5$

$X_A = 3$ $\quad Y_A = 5^3 \bmod 7 = 6$

$X_B = 4$ $\quad Y_B = 5^4 \bmod 7 = 2$

$K = Y_B^{X_A} \bmod 7 = 2^3 \bmod 7 = 1$

$K = Y_A^{X_B} \bmod 7 = 6^4 \bmod 7 = 1$

⑥ Elliptic Curve Cryptography

$y^2 = x^3 + ax + b$

→ Faster and smaller length of keys

ⓐ ECC key exchange

Global public elements:

Eq (a, b)

G: point on EC whose order is large value n.

User A key generation

Select private key $n_a < n$.

Calculate public key $P_a = n_a \times G$

User B key generation

Select $n_B < n$ (Private key)

Calculate $P_B = n_B \times G$.

Calculation of secret key

$K = n_A \times P_B$

$K = n_B \times P_A$

(b) ECC encryption & decryption

Encode M → point m on EC → P_m

For encryption, choose a +ve random int k.

$$CT = C_m = \{kG, P_M + kP_B\}$$

ECC decryption

Multiply 1st point with B's private key

~~$CT = P_m$~~

$$kG \times n_B = kP_B$$

subtract from 2nd point

$$P_M + kP_B - kP_B = \underline{\underline{P_M}}$$

(c) Finding P+Q (VIMP)

$P = (x_1, y_1)$ $Q = (x_2, y_2)$

$P + Q = (x_3, y_3)$ then

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

② Finding 2P (VIMP)

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

* $-P = (x_1, -y)$

→ Zero point : Additive identity : $P + O = P$, $P \neq O$.

→ Sum of 3 points lying on a stright line in an EC = O.

⑦ ECC numerical

Q → On the EC over real number

$$\lambda = \frac{3x_p^2 + a}{2y_p}, \quad x_R = \lambda^2 - x_p - x_q$$

Let P = (3, 10) & q = (9, 7) in $E_{23}(1, 1)$. Find (P+q) & 2P

$$y^2 = x^3 + x + 1 \bmod 23$$

i) $-P = (x, -y) = (3, -10) = (3, 13)$

ii) $(P+q) = (x_3, y_3)$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$= \left(\frac{7-10}{9-3}\right)^2 - 3 - 9$$

$$= \left(\frac{-3}{6}\right)^2 - 12$$

$$= \frac{1}{4} - 12 = 1 \times (4)^{-1} - 12$$

$$= 1 \times 6 - 12 \qquad (\because 4^{-1} = 6)$$

$$= -6 = \underline{17}$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

$$= -10 + \left(\frac{7-10}{9-3}\right)(3-17)$$

$$= -10 + \left(\frac{+1}{2}\right)(+14)$$

$$= -10 + 7$$

$$= -3 = \underline{\underline{20}}$$

$$\therefore (P+q) = (17, 20)$$

iii) $2P = (x_3, y_3)$

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

$$x_3 = \left(\frac{3 \times 9 + 1}{20}\right)^2 - 6$$

$$= \left(\frac{28}{20}\right)^2 - 6$$

~~$= \left(\frac{7}{5}\right)^2 + 17$~~

$$= \left(\frac{\cancel{5}1}{\cancel{20}4}\right)^2 - 6 \qquad (\because 28 = 5 \bmod 23)$$

$$= \left(\frac{1}{4}\right)^2 + 17 \quad = (\times 4^{-1})^2 + 17$$

$$= 6^2 + 17 = 36 + 17 = \underline{7}$$

$$y_3 = -10 + (6)(3 - 7)$$

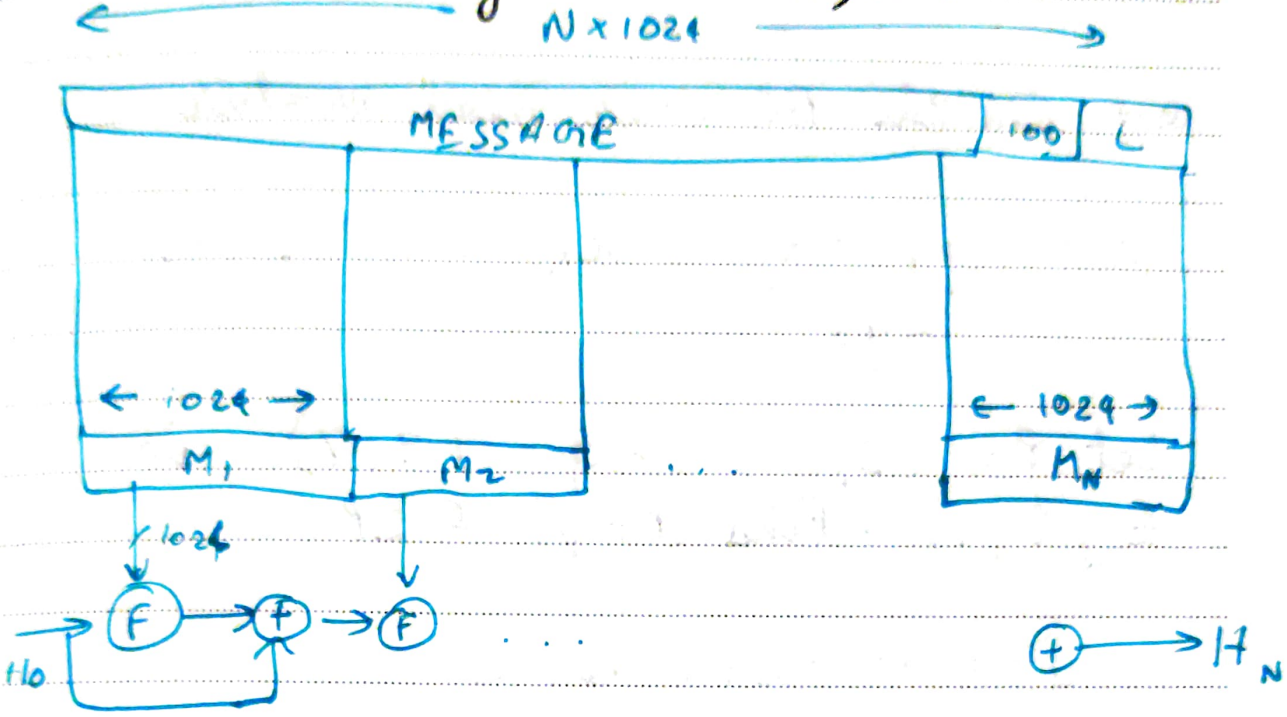
$$= -10 + (6 \times -4)$$

$$= -10 - 24$$

$$= -34 = \underline{12}$$

$\therefore$ $2P = (7, 12)$

⑧ Secure Hash Algorithm (SHA)



Step 1: Append padding bits to make it 896 mod 1024.

Step 2: Append length (128 bit unsigned int)

Step 3: Initialize hash buffer (512 bit buffer)

Step 4: Process message into 1024 bit blocks.
Run it through 80 rounds of f.

Step 5: Output

⑨ Symmetric vs Asymmetric

	Symmetric	Asymmetric
①	One Key	2 keys
②	Private key cryptography	Public key cryptography
③	Faster	Slower
④	Simple	Complex
⑤	Example: DES & AES	Example: RSA & Diffie
⑥	Bulk data transmission	Securely exchanging key.