Unit-3

1) Elgamal Cryptosystems

2) Elliptic curve Cryptography

3) RSA - CO-4

4) Chinese remainder theorem

5) Diffie Hellman Exchange - CO-4

1) diffie - hellman key exchange alg -

→ not an encryption / decryption alg.

→ used to exchange keys b/w sender & receiver

→ Asymmetric key cryptography.

→ Purpose is to enable 2 users to securely exchange a key that can then be used for symmetric encryption messages

⊙ Procedure -

i) Consider a prime no. a

Let $q = 7$

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

Primitive root –

$\alpha^1 \bmod q$

$\alpha^2 \bmod q$

$\alpha^3 \bmod q$

⋮

$\alpha^{q-1} \bmod q$ shld have values in $\{1, 2, 3 \cdots q-1\}$

Eg: $\alpha = 3$ & $q = 7$

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

Here, we have all values from 1 to $q-1$ (ie) 6

So, 3 is a primitive root of 7.

iii) Assume X_A (private key of A) and $(X_A < q)$

Calculate $Y_A = \alpha^{X_A} \bmod q$

X – Private

Y – Public

Eg: $q = 7$ & $\alpha = 5$

and let $X_A = 3$

$Y_A = (5)^3 \bmod 7 = 125 \bmod 7 = 6$

$\boxed{Y_A = 6}$

iv) Assume X_B and $\boxed{X_B < q}$

X_B - Pvt key of B

Y_B - Pub key of B

Calculate $Y_B = \alpha^{X_B} \bmod q$

Let $X_B = 4$

$Y_B = (5)^4 \bmod 7 = 625 \bmod 7 = 2$

$\boxed{Y_B = 2}$

v) Calculate secret key k_1 and k_2 ← for exchanging

k_1 = person A

k_2 = person B

$k_1 = (Y_B)^{X_A} \bmod q$ $\quad$ $k_2 = (Y_A)^{X_B} \bmod q$

after calculating, if $k_1 = k_2$ then success.

$k_1 = (2)^3 \bmod 7 = 8 \bmod 7 = 1$

$k_2 = (6)^4 \bmod 7 = 1296 \bmod 7 = 1$

$\boxed{k_1 = k_2}$

∴ Success

key exchanged successfully.

2) Chinese Remainder theorem - If a no. is divided by several other no. that have no common factors, one can find the remainder when dividing by the product of those no.s

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

Steps:

i) $M = m_1 m_2 m_3$

ii) $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$; $M_3 = \frac{M}{m_3}$

iii) $M_1^{-1} \bmod m_1$ ...

iv) $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots)\bmod M$

Step 1:

$a_1 = 2$ $\quad m_1 = 3$

$a_2 = 3$ $\quad m_2 = 5$

$a_3 = 2$ $\quad m_3 = 7$

Step 2:

$M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 7$

$= 105$

Step 3:

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

Step 4:

~~$M_1^{-1} \bmod m_1$~~

To find: M_1^{-1}:

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

$M_1^{-1} = 35 \bmod 3 = 2$

$3 \mid 35 \mid 11$
-31
05
-2
3

M_2^{-1}:

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod 5$

$M_2^{-1} = 21 \bmod 5 = 1$

M_3^{-1} :

$$M_3 \times M_3^{-1} = 1 \bmod m_3$$

$$15 \times M_3^{-1} = 1 \bmod 7$$

$$M_3^{-1} = 15 \bmod 7 = 1$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$$

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$= 23$$

Now, $23 \equiv 2 \pmod 3$

$23 \bmod 3 \equiv 2 \pmod 3$

$2 \equiv 2$ ✓

$23 \equiv 3 \pmod 5$

$23 \bmod 5 \equiv 3 \bmod 5$

$3 \equiv 3$ ✓

$23 \equiv 2 \pmod 7$

$23 \bmod 7 \equiv 2 \bmod 7$

$2 \equiv 2$ ✓

4	With a neat sketch explain the Elliptic curve cryptography with an example	10	K2	CO4
5	Explain DiffieHellman algorithm and find the secret key shared between user A and user B using DiffieHellman algorithm for the following q=353; α (primitive root)=3, XA=45 and XB=50	10	K2	CO4
6	Users A and B use the Diffie-Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. (i) If user A has private key XA=3.What is A's public key YA? (ii)If user B has private key XB=6. What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm.	10	K2	CO4
7	Explain in detail about Elgamal Cryptosystems.	10	K2	CO4
	Explain Chinese Remainder theorem and find X for the given set of congruent equation using CRT	10	K3	CO3

⊙ Diffie - Hellman algorithm -

$q = 353$ (prime no)

$\alpha = 3$

$x_A = 45$

$x_B = 50$

} → given.

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

$= 3^{45} \bmod 353 = \quad \bmod 353 = 143$

$Y_B = = \alpha^{x_B} \bmod q$

$= 3^{50} \bmod 353 = \quad \bmod 353 = 155$

ii) $K_A = Y_B^{x_A} \bmod q = 155^{45} \bmod 353 = 197$

$K_B = Y_A^{x_B} \bmod q = 143^{50} \bmod 353 = 197$

Gn - both users have same shared secret.

$K_A = K_B$

∴ key = 197

1) Elliptic Curve Cryptography.

→ It is asymmetric public key cryptosystem

→ It provides equal security with smaller key size as compared to ~~RSA~~ non ~~encryption~~ elliptic curve cryptography algorithm.

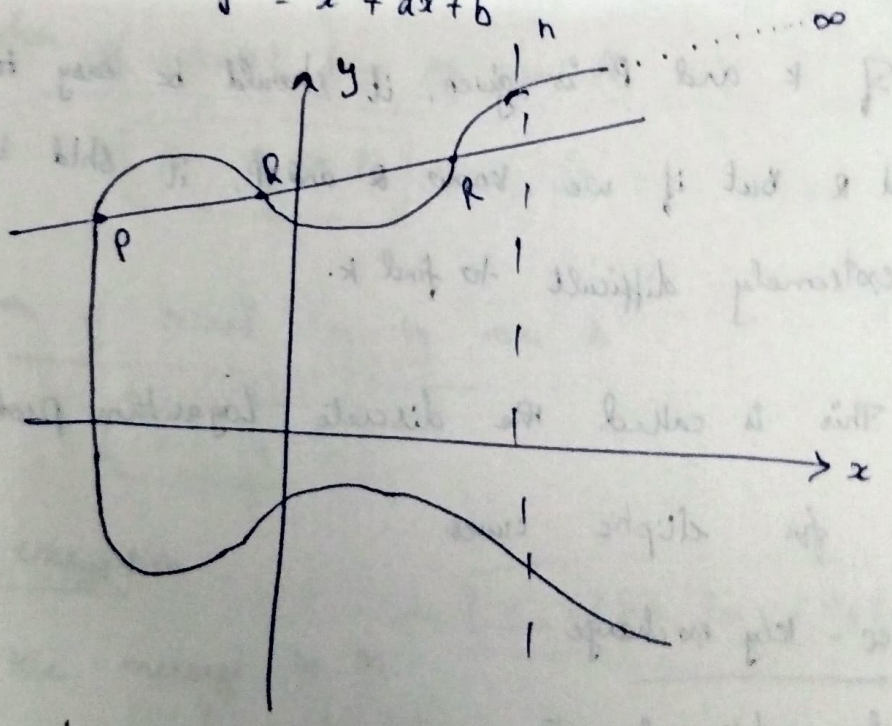
(ie)

Small key size and high security

→ It makes use of elliptic curves

→ Elliptic curves are defined by some mathematical functions - cubic function.

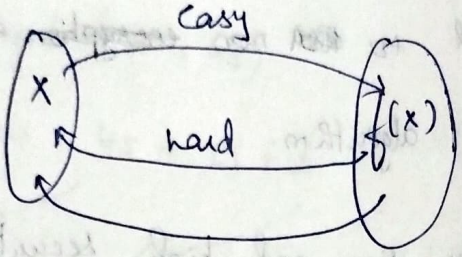
$$y^2 = x^3 + ax + b$$



→ Symmetric to x-axis

→ If we draw a line, it will touch a max of 3 points

→ A trapdoor function is a fn that is easy to compute in one direction, yet difficult to compute in the opposite direction without special info, called the trapdoor.



easy if given "t" → trapdoor value

- Let $E_p(a, b)$ be the elliptic curve.
- Consider the equation $Q = kP$

  where, Q, P → points on curve and $k < n$.
- If k and P is given, it should be easy to find Q but if we know Q and P, it shld be extremely difficult to find k.
- This is called the discrete logarithm problem for elliptic curves.

⊙ ECC - key exchange

global public elements

$E_q(a,b)$: elliptic curve with parameters a, b and q

→ q is prime no. or an integer of the form 2^m.

G : Point on the curve / elliptic curve whose order is large value of n.

User A key generation

Select private key n_A $\quad n_A < n$

calculate public key P_A $\quad \boxed{P_A = n_A \times G}$

User B key generation

Select private key n_B $\quad n_B < n$

Calculate public key P_B $\quad \boxed{P_B = n_B \times G}$

Calculation of secret key by user A

$$\boxed{K = n_A \times P_B}$$

Calculation of secret key by user B

$$\boxed{K = n_B \times P_A}$$

⊙ Ecc encryption.

→ Let the message be M $\quad \leftarrow \boxed{Cm = \{kG, Pm + kP_B\}}$

→ First encode this message M into a point on elliptic curve.

⊙ ECC decryption -

→ for decryption, multiply 1st point in the pair with receivers secret key.

ie $k_G * n_B$

$= P_m + kP_B - (k_G * n_B)$

$= P_m + kP_B - kP_B$

$= P_m$ (original point

→ receiver gets the same point.

2) Elgamal Encryption Algorithm -

→ It is a public key cryptosystem.

→ It uses asymmetric key encryption to communicate b/w two parties and encrypt the message.

→ It is done in 3 steps - i) key Generation
ii) Encryption
iii) Decryption

i) key Generation:

→ Select large prime number (p) = p = 11

→ Select a decryption key also called private key.

d = 3

→ Select second part of encryption key $(e_1) = 2$

$\boxed{e_1 = 2}$

→ Calculate 3rd part of encryption key (e_2)

$$e_2 = e_1^d \bmod p$$

$$= (2)^3 \bmod 11$$

$$= 8 \bmod 11$$

$\boxed{e_2 = 8}$

→ Public key = (e_1, e_2, p) and private key = d

$\boxed{\text{Public key} = (2, 8, 11)}$

$\boxed{\text{Private key} = 3}$

ii) Encryption -

→ Select random integer (R)

$\boxed{R = 4}$

→ Calculate $c_1 = e_1^R \bmod p$

$$= 2^4 \bmod 11$$

$$= 16 \bmod 11$$

$\boxed{c_1 = 5}$

→ Calculate $c_2 = (PT \times e_2^R) \bmod p$, assume $PT = 7$

$$= (7 \times 8^4) \bmod 11$$

$$= 28672 \bmod 11$$

$\boxed{c_2 = 6}$

→ Cipher text, $(C_1, C_2) = (5, 6)$

iii) Decryption -

→ $PT = [C_2 \times ((C_1)^D)^{-1}] \bmod P$

$= [6 \times ((5)^3)^{-1}] \bmod 11$

$= 6 \times (5^3)^{-1} \bmod 11$

$= 6 (125)^{-1} \bmod 11$

Solve, $(125)^{-1} \bmod 11$

$\Rightarrow 125 \times x \bmod 11 = 1$

Let $x = 1 \Rightarrow 125 \bmod 11 \neq 1$

$x = 2 \Rightarrow 125 \times 2 \bmod 11 = 250 \bmod 11 \neq 1$

$x = 3 \Rightarrow 125 \times 3 \bmod 11 = 375 \bmod 11$

$= 1$

$\therefore x = 3$

$= 6 \times 3 \bmod 11$

$= 18 \bmod 11$

$= 7$

Plain text = 7

$\therefore$ LHS = RHS

Correct answer.

⊙ Applications -

→ Encryption

→ digital Signatures

⊙ Advantages -

→ Security

→ key distibution

→ Digital Signatures

⊙ Disadvantages -

→ Slow processing

→ Key size

→ vulnerability to certain attacks.