Module-4

Asymmetric key Cryptography:

- **Principal of public key cryptosystems:**

The principales of public key cryptosystem revolves around the use of asymmetric cryptography.

- **Public key:-** Used for encryption or Signature verification, know to everyone
- **Private key:-** Used for decryption or Signature creation; known only to the owner
- **key Distribution:-** Unlike symmetric systems, public key system simplify secure key distribution since the public key can be openly shared.
- **Authentication:-** A Sender can sign a message using their private key. Anyone can verify it using the public key proving the sender's identity.
- **Non-Repudiation:-** Once a message is signed with a private key, The sender cannot deny sending it, Because only their private key could created the signature.

Quick Work
Page No.:
Date:
M T W T F S S

RSA [Ron Rivest, Adi Shamir, Leonard Adleman

- Algorithm.

Select p, q ---- p, q both prime & p ≠ q

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1) \times (q-1)$

Select e such that i] $GCD(\phi(n), e) = 1$ } and
ii] $1 < e < \phi(n)$

Calculate d : $d \times e \bmod \phi(n) = 1$

Public key = $\{e, n\}$

Private key = $\{d, n\}$.

Example $p = 3$ $q = 5$ $\therefore n = p \times q = 15$

$\phi(n) = (p-1) \times (q-1) = 2 \times 4 = 8$

Compute e such that $GCD(e, \phi(n)) = 1$ & $1 < e < \phi(n)$.

$\therefore e = \{3, 5, 7\}$.

Let $e = 3$

$\therefore d \times e \bmod \phi(n) = 1 \Rightarrow d \times 3 \bmod 8 = 1$

$\therefore d = 3$

Public key = $\{e, n\} = \{3, 15\}$

Private key = $\{d, n\} = \{3, 15\}$.

$C = M^e \bmod n$ $\quad$ $M = C^d \bmod n$

Quick Work
Page No.:
Date:
M T W T F S S

Applications of RSA.

- Digital Communication.
- Data Security.
- Digital Transactions.

Advantages of RSA.

1] Highly Secure when used with sufficient High long Key length.

2] Dual-key System in RSA eliminates the need for both parties to share a secret key beforehand.

3] Used in Secure Communication and document

4] RSA is based on the mathematical difficulty of factoring large Semiprime Numbers. which is believed to be a hard problem.

5] RSA has been widely standardized and is supported by many cryptographic libraries & Software implementation.

Disadvantages of RSA.

1] key lengths can impact performance and increase computational overhead.

2] Encryption and decryption operations are computationally intensive.

3] It could be broken by Quantum computing.

4] RSA key management can be challenging.

5] Lack of Forward Secrecy.

Attack on RSA:

1] Brute Force Attack [Not Practical for large key

2] Mathematical Attack:
   a. Factoring the Modulus.
      ↳ The security of RSA depends on the difficulty of factoring large Number; General Number field Sieve are used.
   b. Small private Exponent attack
      ↳ If the private keey d is too small, it can be Recoverd using Continued fractions.

3] Timing Attack.
   ↳ Based on How long it takes to perform decryption or Signature operation.

4] Chosen Ciphertext Attack.
↳ The attacker Submit chosen ciphertext to the decryption and analyze the Result.

Countermeasure: Use padding scheme.

5] Chosen plaintext Attack.
↳ If an attacker can encrypt arbitrary message, They may infer pattern or Relationship

6] Side channel attack.
↳ Use physical data during decryption to Recover key.

* How to make RSA Strong?

1] Use Strong key Length.

2] Employ Secure padding scheme.

3] Regularly update cryptographic libraries

4] Follow best practice in key management.

5] Actively explore post-quantum cryptographic alternatives.

6] Use padding in Message Text.

Quick Work
Page No.:
Date:
M T W T F S S

ECC [Elliptic Curve Cryptography].

- Branch of public key cryptography.
- Based on the mathematical properties of elliptic curve.
- Elliptic Curve are mathematical curve defined by

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

ECC vs RSA.

1] Strong key with Smaller key
   ↳ ECC 256-bit ≈ RSA 3072-bit Security level.
   This leads to : 1] Faster Computation
   2] Reduced power Consumption
   3] less Memory Usage.

2] Performance Efficiency.
   ↳ Faster key generation, Encryption/decryption and signing.
   Ideal for Resource constrained environment : Mobile devices
   IOT devices
   Smart cards.

3] Better for Morden Protocols.
   ↳ widely adopted in morden cryptographic protocols : TLS
   SSH
   Bitcoin & other Cryptocurrencies.

Quick Work
Page No.:
Date:
M T W T F S S

ECC example.

Given Elliptic Curve : $E_{11}(1,6)$ find matching points on curve over Z_p.

→ $E_{11}(1,6)$ i.e. $p=11$ $a=1$ $b=6$.

$\therefore y^2 \bmod 11 = x^3+x+6 \bmod 11$.

x, y	$x^3+x+6 \bmod 11$	$y^2 \bmod 11$.
0	6	0
1	8	1
2	5	4
3	3	9
4	8	5
5	4	3
6	8	3
7	4	5
8	9	9
9	7	4
10	4	1

(2,4) (2,7) (3,5) (3,6) (5,2) (5,9) (7,2) (7,9) (8,3) (8,8) (10,2) (10,9).

Quick Work
Page No.:
Date:
M T W T F S S

Addition over E_p.

→ Compute Slope between P and Q :

$$\lambda = \frac{y_q - y_p}{x_q - x_p} \bmod p. \quad \Rightarrow \quad P \neq Q.$$

$$\lambda = \frac{3x_p^2 + a}{2y_p} \bmod p.$$

→ Calculate the Sum R.

$$x_r = \lambda^2 - x_p - x_q \bmod p$$
$$y_r = \lambda \times (x_p - x_r) - y_p \bmod p.$$

Given $P = (3, 10)$ $Q = (9, 7)$ over $E_{23}(1, 1)$.
Find $P + Q$.

$P \neq Q \quad \therefore \lambda = \frac{7-10}{9-3} = -\frac{1}{2} \bmod 23$

$a = 1 \quad b = 1 \quad p = 23.$

$$x_r = \lambda^2 - x_p - x_q \bmod 23 = \left(\frac{-1}{2}\right)^2 - 3 - 9 = -\frac{47}{4}$$

$$= -\frac{47}{4} \bmod 23$$

Given $P(3,10)$ $Q=(9,7)$ $E_{23}(1,1)$ Compute $P+Q$.

$P = 23 \quad a=1 \quad b=1$.

Here $P \neq Q$.

$\therefore \lambda = \frac{y_p - y_q}{x_p - x_q} \bmod 23$

$= \frac{7-10}{9-3} = \frac{-1}{2} \bmod 23.$

$= (1 \bmod 23 \times (-2^{-1} \bmod 23)) \bmod 23$

$= (1 \times -12) \bmod 23$

$= -12 \bmod 23 = 11$

$x_r = \lambda^2 - x_p - x_q = 11^2 - 3 - 9 = 109 \bmod 23$

$= 17$

$y_r = \lambda - (x_p - x_r) - y_p \bmod 23$

$= 11 * (3 - 17) - 710 \bmod 23$

$= 11 * (-14) - 10 \bmod 23$

$= -164 \bmod 23 = 20$

$y_r = 20$

$P + q = (17, 20)$