R.SA Algorithm

Rivest - Shamir - Adleman developed in 1978

→ It is an asymmetric cryptographic algo. (2 keys) ie public and private key concept is used here.

→ The [acronym RSA] is made from the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman.

→ Public key → known to all users in N/W
Private key → kept secret, not sharable to all.

... used for encryption,

Algorithm

Rivest - Shamir - Adleman developed in 1978

→ It is an asymmetric cryptographic algo.
(2 keys) ie public and private key concept is used here.

→ The [acronym RSA] is made from the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman.

→ Public key → known to all users in N/W
Private key → kept secret, not sharable to all.

If public key of user A is used for encryption, we have to use the private key of same user for decryption.

The RSA scheme is a $\boxed{\text{block cipher}}$ in which the plain text and ciphertext are integers b/w 0 and n-1 for some value n.

RSA Algorithm in Cryptography and Network Security

1.75

1. Key Generation

(i) select 2 $\boxed{\text{large}}$ prime nos 'p' and 'q' → for higher security.

(ii) calculate $n = p * q$

(iii) calculate $\phi(n) = (p-1) * (q-1)$ // eulers Toitient f^n

(iv) choose value of e

$$1 < e < \phi(n) \text{ and } \gcd(\phi(n), e) = 1$$

(v) calculate

$$d \equiv e^{-1} \bmod \phi(n)$$

ie $ed \equiv 1 \bmod \phi(n)$ → $ed \bmod \phi(n) = 1$

(vi) public key $= \{e, n\}$

(vii) private key $= \{d, n\}$

Plaintext $= \underline{M < n}$ imp

Encryption

// c → ciphertext

3:51 / 10:14

Let $p = 3, q = 11$

$n = p * q = 3 * 11 = 33$

$\phi(n) = 2 * 10 = 20 \quad \because \phi(n) = (p-1)(q-1)$

So, let $\boxed{e = 7}$ as $1 < 7 < 20$ and $gcd(7, 20) = 1$

Now, $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n) \longrightarrow de \bmod \phi(n) = 1$

$7 * d \equiv 1 \bmod \phi(n)$

$(7 * d) \bmod 20 = 1 \quad (\because d = 3)$

multiplicative inverse of 7

// find multiples of $\phi(n)$ ie here 20, and just find a no. satisfying a value greater than this ie $(7*d)$ should be 21.

We can solve it using extended euclidean algorithm also

in next video (I will use this method).

ie $e = 7, d = 3$

$\{e, n\} = \{7, 33\}$

Key Generation

select 2 $\boxed{\text{large}}$ prime nos 'p' and 'q' → for higher security.

calculate $n = p * q$

) calculate $\phi(n) = (p-1) * (q-1)$ // eulers Toitient f^n

) choose value of e

$1 < e < \phi(n)$ and $gcd(\phi(n), e) = 1$

) calculate

$d \equiv e^{-1} \bmod \phi(n)$

ie $ed \equiv 1 \bmod \phi(n) \rightarrow ed \bmod \phi(n) = 1$

) public key $= \{e, n\}$

) private key $= \{d, n\}$

2. **Encryption**

Plaintext $= M < n$ imp

$C = M^e \bmod n$ // $C \rightarrow$ ciphertext

3. **Decryption**

$M = C^d \bmod n$

$(7*d) \bmod 20 = 1$ $\quad (\because d = 3)$

multiplicative inverse of 7

multiples of $\phi(n)$ ie here 20, and just
uid a no. satisfying a value greater
than this ie $(7*d)$ should be 21.

solve it using extended euclidean
ithm also

in next video
(I will use this
method).

$= 7,\ d = 3$

ey $= \{e, n\} = \{7, 33\}$

key $= \{d, n\} = \{3, 33\}$

ON $\quad$ let $m = 31$

$C = M^e \bmod n$

$C = 31^7 \bmod 33 = 4 \quad \rightarrow \boxed{C = 4}$

N

$M = C^d \bmod n = 4^3 \bmod 33 = 31$

$\boxed{m = 31}$

(ii) calculate $n = p*q$ ... and q

(iii) calculate $\phi(n) = (p-1)*(q-1)$ // eulers Toitient f^n

(iv) choose value of e

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

(v) calculate

$d \equiv e^{-1} \bmod \phi(n)$

ie $\quad ed \equiv 1 \bmod \phi(n) \rightarrow ed \bmod \phi(n) = 1$

(vi) public key $= \{e, n\}$

(vii) private key $= \{d, n\}$

2. Encryption $\quad$ Plaintext $= M < n$ imp

$C = M^e \bmod n$ $\quad$ // C → ciphertext

3. Decryption $\quad$ Abhi → 4

$M = C^d \bmod n$

Note → (e, n) is public key used in encryption

(d, n) → private key used for decryption