RSA Algorithm

=> The acronym RSA is made from the initial letters of the surnames of:
Ron Rivest, Adi Shamir and Leonard Adleman

=> RSA algo was developed in 1978

=> It is an asymmetric algorithm using 2 keys
i.e public key and private key

=> Public Key:
Key know to all users in network

=> Private key:
Kept secret, not shared to all

=> If public key of user A is used for encryption then we have to use the private key of same user for encryption

=> The RSA algo is a Block cipher in which the plain txt and cipher txt are integers blw 0 and n-1 for some value of 'n'

Algorithm

1- Key Generation

(i) Select 2 large prime number as 'p' and 'q'

(ii) calculate $n = p * q$

(iii) calculate $\phi(n) = (p-1) * (q-1)$

$\because \phi$ = euler's totient function

(iv) Choose value of 'e'

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

(v) Calculate

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

i.e $ed \equiv \text{Mod } \phi(n)$

$ed \text{ Mod } \phi(n) \equiv 1$

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

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

2- Encryption

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

∵ C = value calculated in key gen method

∵ C = cipher txt

M = Plain txt

∵ M = no of integers/digits in plain text and it should be $M < n$

e.g Plain txt = Abhi

so M = 4

3- Decryption

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

∵ M = plain txt

∵ d = calculated in key Gen Method

∵ Cipher txt

Note:

Public key {e, n} is used in encryption process

so

Private key {d, n} is used in decryption process.

Example

We are supposed to take some large prime numbers but for the sake of example we'll take small number

$p = 3, q = 11$

(ii) $n = p * q = 3 \times 11$

$\boxed{n = 33}$

(iii) $\phi(n) = (p-1) * (q-1)$

$= (2) * (10)$

$\boxed{\phi(n) = 20}$

(iv) chose value of e

let $e = 7$

so $1 < 7 < 20 \Rightarrow (T)$ and $\gcd(7, 20) = 1$

(v) now

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

$de \bmod \phi = 1$

$(7 * d) \% 20 = 1$

$\therefore 21 \% 20 = 1$

so $\boxed{d = 3}$

$(7 * 3) \% 20 = 1 \Rightarrow (T)$

20 → 21 | 21*20=1
40 → 41
60 → 61
80 → 81

(vi) Private key = (d, n)

(vii) Public key = (e, n)

Encryption

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

Let $M = 31$ so

$M < n$, $31 < 33 = \phi(T)$

$$C = (31)^7 \bmod 33$$

$$\boxed{C = 4}$$

Decryption

$$M = C^d$$

$$= 4^3 \bmod 33$$

$$\boxed{M = 31}$$

Diffie-Hellman Key Exchange

=> It is not an encryption algorithm.
=> It is used to exchange secret keys between ...2 users.

➔ We will use a symmetric encryption to exchange the secret keys b/w users.

➔ We use this algorithm bcz when we are sending a key to reciever, transition it can be attacked in b/w. algorithm.

Algorithm

(i) consider a prime number 'q'

(ii) select α such that it must be the primitive root of q and $\alpha < q$

α is a primitive root if

$\alpha \bmod q$
$\alpha^2 \bmod q$
$\alpha^3 \bmod q$
$\alpha^{q-1} \bmod q$

gives result within = {1, 2, 3, ... q-1}

Example let $q = 7$

$5^1 \bmod 7 = 4$

$5^2 \bmod 7 = 6$ $= \{1, 2, \ldots 6\}$

$5^3 \bmod 7 = 2$ $=$

$5^4 \bmod 7 = 3$ $= \{1, 2, 3, \ldots q-1\}$

$5^6 \bmod 7 = 1$

So we can take 5 as α and it satisfies both condition

(i) it is primitive root of 7

(ii) $5 < 7 \Rightarrow$ (T)

(iii)

$\therefore X \rightarrow$ private key of user

$\therefore Y \rightarrow$ public key of user

assume X_A (private key of A) and $X_A < q$.

calculate

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

(iv)

assume X_B (private key of B) & $X_B < q$

calculate

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

Now we will calculate Secretes keys

=> To calculate the secret keys both sender and receiver will use public keys

$$K_1 = (Y_B)^{X_A} \bmod q$$

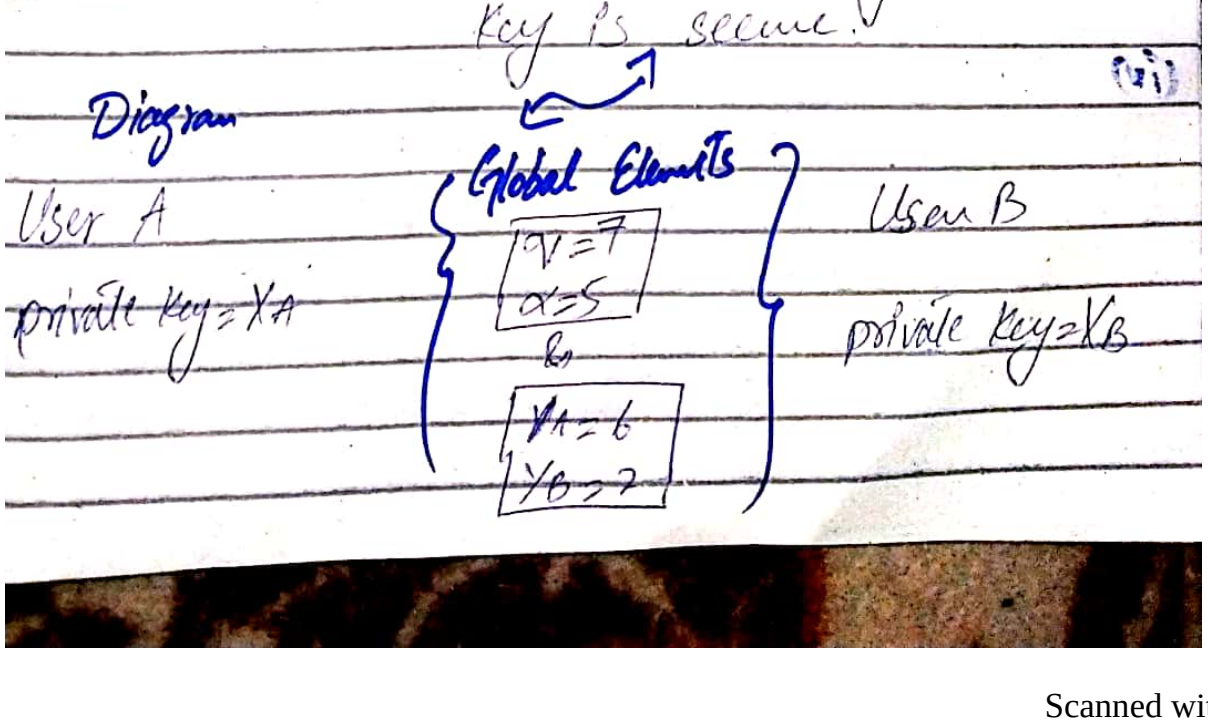
∴ K_1 = Key of user A
∴ X_A = Private key of user A
∴ Y_B = Public " " B

$$K_2 = (Y_A)^{X_B} \bmod q$$

∴ K_2 = Key of user B
∴ X_B = Private key of " "
∴ Y_A = Public " " " "

If $K_1 = K_2$
then we can say that Key is secure.

Diagram



Example

(i) $q = 7$

(ii) $\alpha = 5$

$\Rightarrow \alpha$ is primitive root — (T)

$\Rightarrow \alpha < q$ — (T)

$\Rightarrow$ we can also take 3 as 'α'

(iii)

Assume $X_A = 3$

so

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

$= 5^3 \bmod 7$

$Y_A = 6$

(iv)

Assume $X_B = 4$

so

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

$= 5^4 \bmod 7$

$Y_B = 2$

Secret key Calculation

(P1)

$K_1 = (Y_B)^{X_A} \bmod q$

$= 2^3 \bmod 7$

$K_1 = 1$

(P2)

$K_2 = (Y_A)^{X_B} \bmod q$

$= 6^4 \bmod 7$

$K_2 = 1$

$\Rightarrow$ Keys K_1 & K_2 are succesfully exchanged