02 February 2021
10:07

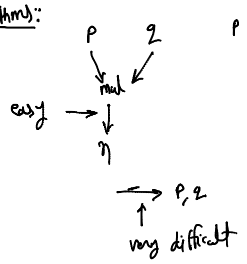
Public key cryptography: (Asymmetric cryptography)

K_{PR}, K_{PU} — Sender

K_{PR} K_{PU} — Receiver

RSA Algorithm:

p & q are two prime number



RSA encryption: $c = m^e \bmod n$

RSA Decryption: $m = c^d \bmod n$

c: cipher text
m: plain text
e, d, n

Receiver (K_{PU_B}, K_{PR_B}) — key generation
- private key = (d, n)
- public key = (e, n)

Key generation in RSA (e, n) (d, n)

1. select two prime numbers p & q
2. Calculate $n = p \times q$
3. calculate $\phi(n) = (p-1) \times (q-1)$
4. choose a value for e, such that $1 < e < \phi(n)$ && $\gcd(\phi(n), e) = 1$
5. Calculate $d = e^{-1} \bmod \phi(n)$
   $[\because (d * e) \bmod \phi(n) = 1]$
6. Private key = P_R = (d, n)
   public key = P_U = (e, n)

Exam ① Let $p = 3$, $q = 11$

② $n = 3 \times 11 = 33$

③ $\phi(n) = (3-1) \times (11-1) = 20$

④ Let $e = 3$

$\phi(n) = 20 = 2 \times 2 \times 5$

$\because 1 < 3 < 20$ ✓

$\because \gcd(3, 20) = 1$ ✓

⑤ $d = e^{-1} \bmod \phi(n)$

$\because d \cdot e = 1 \pmod{20}$

Let $d = 7$, $3 \times 7 = 1 \pmod{20}$ ✓

⑥ Private key K_{PR} = ~~(7, 20)~~ = (7, 33)

public key K_{PU} = (3, 20) = (3, 33)

02 February 2021
10:51

RSA : Plaintext $M <= n$

Encryption function in RSA

$\Rightarrow C = m^e \bmod n$

Receiver

PU = (3, 33) | PR(7, 33)

Key generation

PR PU

Exa. Let $M = 31$,

Sender side

So cipher text $C = 31^3 \bmod 33$

$= 29791 \bmod 33$

$= 29791 - 33 \times 902$

$= 25$

Cipher = 25

Receiver side

Cipher = 25, $d = 7$, $n = 33$

$P \Rightarrow C^d \bmod n$

$\Rightarrow 25^7 \bmod 33$

$\Rightarrow 6103515625 \bmod 33$

$P \Rightarrow 31$

Q.2 In a RSA cryptosystem, a participant A uses two prime number $P = 13, Q = 17$ to generate his public & private key. if the public key of A is 35 then the private of A = ?

given, $P = 13, Q = 17$

$n = 13 \times 17 = 221$

$\phi(n) = (13 - 1) \times (17 - 1) = 192$

given $e = 35$

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

$d = 35^{-1} \bmod \phi(n)$

Diffie Hellman Algorithm:

(Public Key cryptography) used to sharing the key via insecure channel.

Algorithm work in following steps.

A [Sender] [Receiver] B

Algorithm work in following steps. A [sender] [Receiver] B

① Global public element:

q : Prime number

α : $\alpha < q$ And α is primitive root of mod q.

② A's key generation:

[select Private key X_A : $X_A < q$

[calculate Public key Y_A : $Y_A = \alpha^{X_A} \bmod q$

③ B's key generation

[select Private key $X_B < q$

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

④ Secrete key calculation By A (sender) : $K = (Y_B)^{X_A} \bmod q$

Secrete Key calculation By B (Receiver): $K = (Y_A)^{X_B} \bmod q$

Primitive root:

if an integer (a) has order $\phi(n) \bmod n$

(where n is positive number (integer) and GCD $(a, n) = 1$

then a is Primitive root of n, such that

$$a^{\phi(n)} \equiv 1 \pmod n$$

Eg. find the primitive root of 6.

Sol.

$n = 6$

$\phi(n) = \phi(6) = \phi(3 \times 2) = (3-1) \cdot (2-1) = 2$

$a^{\phi(n)} \equiv 1 \pmod n$, $a^2 \equiv 1 \pmod 6$

possible value of $a = 2, 3, 4, 5$

Let select $a = 5$ $5^2 \pmod 6 \equiv 1$

$25 \bmod 6 \equiv 1$

Let select $a = 4$ $4^2 \pmod 6$

$16 \pmod 6 = 4$ ✗

Eg. ② find Primitive root of 10

Sol

$n = 10$

$\phi(n) = \phi(10) = \phi(5 \times 2) = (5-1) \cdot (2-1)$

$= 4$

$a^{\phi(n)} \equiv 1 \pmod{10}$

possible number for $a = 3, 5, 7$

Let $a=3$, $3^4 \pmod{10} \Rightarrow 81 \bmod 10 \Rightarrow 1$

Let $a=5$, $5^4 \pmod{10} \Rightarrow \Rightarrow 5$

Let $a=7$ $7^4 \pmod{10} \Rightarrow 7\times7\times7\times7$

$49 \quad 49$

$(49 \bmod 10) \cdot (49 \bmod 10)$

$9 \cdot 9$

$(81) \bmod 10 \Rightarrow 1$

So 3 & 7 are Primitive root of 10.

Q. find Primitive root of 15.

Sol. $n=15$

$\phi(n) = \phi(15) = \phi(5\times3) = (5-1)(3-1) = 4\times2 = 8$

Let $a=2$, $2^8 \equiv 1 \bmod (15)$, $256 \bmod 15 = 1$

Q. Let $q=7$ then find public Private Key for sender & Receiver & evaluate secret Key by both.

$\phi(n) = (7-1) = 6$

Sol. $q=7$

$\alpha = ?$ let $\alpha=5$ | let $\alpha=3$

$a^{\phi(n)} \equiv 1 \bmod$

$2^6 \bmod 6 = 1$

$3^6 \bmod 6 = 1$ ✓

$4^6 \bmod 6 = 1$

$5^6 \bmod 6 = 1$ ✓

A's Key: $X_A = 3$

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

B's Key: $X_B = 4$

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

secrete key (A) $= Y_B^{X_A} \bmod 7 = 2^3 \bmod 7 = 1$

secrete key (B) $= Y_A^{X_B} \bmod 7 = 6^4 \bmod 7 = 1$