2021

UNIT-II PUBLIC KEY ~~CRR~~ CRYPTOGRAPHY AND RSA ALGORITHM.

Public Key Cryptography :
- also called as two-key/asymmetric.

Characteristics :
1. Infeasible to determine the decryption key using the knowledge of algorithm and encryption key.
2. Either of 2 keys can be used for encryption while the other is used for decryption

- There are 2 keys : public key, private key.

$A \rightarrow B$

$A \rightarrow PU_A, PR_A$ $B \rightarrow PU_B, PR_B$

Encry → Public   Decryp → Private

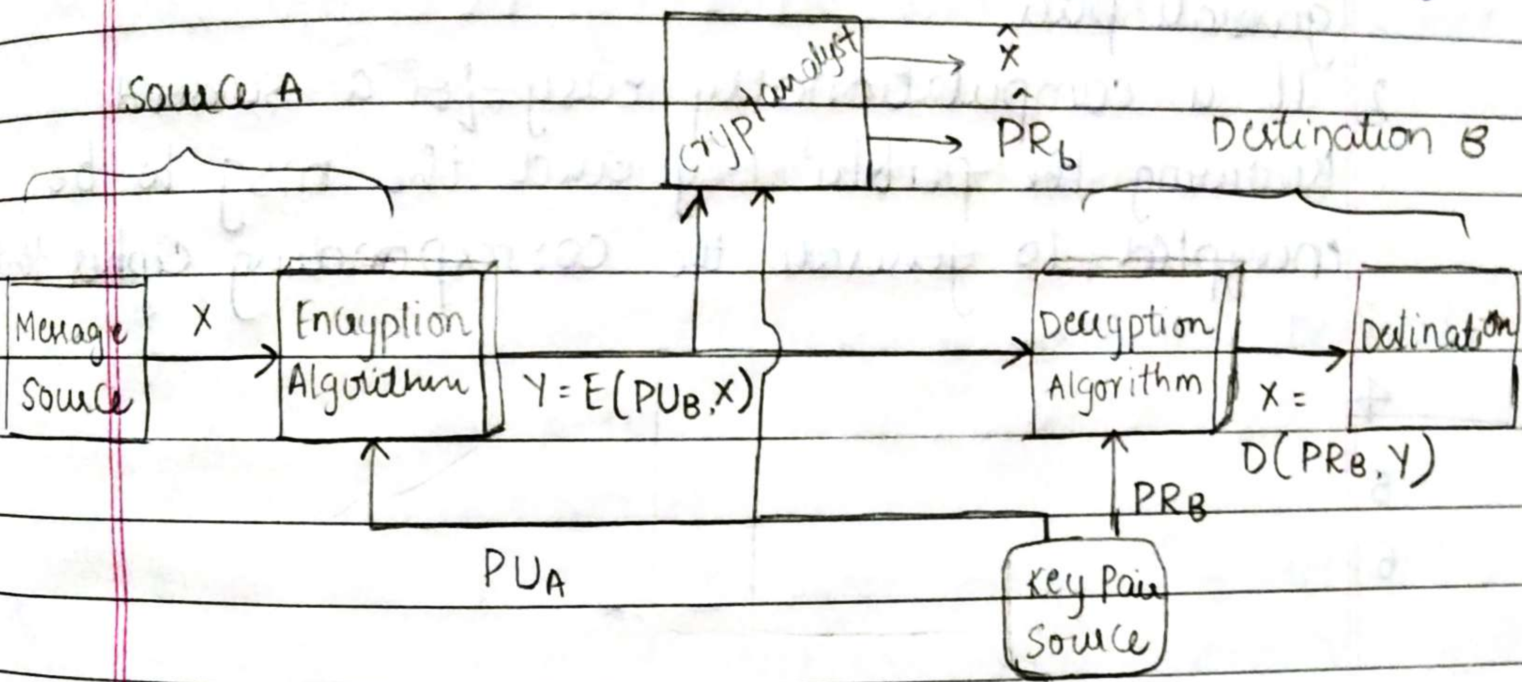
Encry → PU_A Decry → PR_A

Encry → PR_B Decry → ~~PRB~~ PU_B

Ingredients of Public Key encryption.
1. Plain text
2. Encryption Algo
3. Public Key
4. Private Key
5. Decryption Algo
6. Cipher Text.

- It is used to provide secrecy and authenticat^n

Public Key cryptosystem to provide secrecy



To provide authentication
Encrypt using private key of sender
decrypt " public " "

To provide secrecy and authentication we do double encryption & double decryption.

Applications for Public Key Cryptography
- 3 categories.

1. Encryption / Decryption — RSA, Elliptic curve.
2. Digital Signature — Defi Helman
3. Key exchange. — DSS

2021

Requirements for Public Key Cryptography

1 It is computationally very easy for a party B to generate pair

2 It is computationally easy for a sender A knowing the public key and the msg to be encrypted, to generate the corresponding cipher text

3

4

5

6

Trap-door one way function

One way funct^n

- Computation of function is easy
  $Y = f(x)$ is easy
- computation of inverse is infeasible
  $X = f^{-1}(Y)$ infeasible

For trap door one way funct^n :

$Y = fK(X)$ easy, if K and X are known

$X = fK-1(Y)$ easy, if K and Y are known

$X = fK-1(Y)$. if Y is known and K is known .

-2021

Public Key Cryptanalysis :

RSA Algorithm

- Developed in 1977 by Ron Rivest, Adi Shamir and Len Adleman
- RSA - Rivest Shamir Adleman

- Makes use of an expression with exponentials.

C = M^e mod n

M = C^d mod n

e, d are keys used for encryptⁿ & decryptⁿ

Both sender and receiver shld know value of n.

Public Key = {e, n} Private key = {d, n}

Requirements :

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

$M = C^d \bmod n$

$= (M^e)^d \bmod n$

$= M^{ed} \bmod n$

$ed \bmod \phi(n) = 1$

Steps :

1. Find 2 large prime no.s p, q
2. $n = pq$ is calculated
3. $\phi(n) = (p-1)(q-1)$
4. Select 'e' such that $\gcd(e, \phi(n)) = 1$
5. Calculate 'd' such that $d \equiv e^{-1} \pmod{\phi(n)}$
6. Public key $\rightarrow (e, n)$
7. Private key $\rightarrow (d, n)$
8. $C = M^e \bmod n$
9. $M = C^d \bmod n$

Eg : $p = 3 \quad q = 5 \quad M = 2$

$n = pq = 15$

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

$= 2 \times 4 = 8$

Value of e should be $1 < e < \phi(n)$

Let $e = 3$

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

$$d = \frac{1 + k\phi(n)}{e} \Rightarrow \frac{1 + k(8)}{3}$$

for $k = 1$, $\frac{1+8}{3} = \frac{9}{3} = 3 \Rightarrow d$

$C = M^e \bmod n$

$= 2^3 \bmod 15$

$= 8 \bmod 15 = 8$

$M = C^d \bmod n$

$= 8^3 \bmod 15 = 512 \bmod 15$

$= 2$

RSA to process multiple blocks of data

a - z (00 - 25)

A - Z (26 - 51) 28720958.12

10-4-2021

Computational Aspects

1 Encryption / Decryption

1st method : $88^{11} \bmod 187$ $88^{11} = \_\_\_ \times 10^{-}$

so we break down 88 without getting 10^{-}

eg: $88^5 = 5277319168$ with no 10^{-}

so $(88^5 \bmod 187) \times (88^5 \bmod 187) \times (88^1 \bmod 187)$

$= (88^{11} \bmod 187)$

$\therefore$

$(22 \times 22 \times 88) \bmod 187 = 143$

$\therefore 88^{11} \bmod 187 = 143$

2^{nd} method : Algorithm for computing $a^b \bmod n$

$88^{11} \bmod 187$ 11 binary representatⁿ = $\overset{3}{1}\overset{2}{0}\overset{1}{1}\overset{0}{1}$

$a = 88$ $b = 11$ $n = 187$

$c = 0$ $f = 1$

for $i = 3$

$C = 2 \times c = 0$

$f = (1 \times 1) \bmod 187 = 1$

if $b_3 = 1$ 'Y'

$c = C + 1 = 1$

$f = (f \times a) \bmod n$

$= (1 \times 88) \bmod 187$

$= 88$

$C = 1$ $f = 88$

for $i = 2$

$C = 2$

$f = (88 \times 88) \bmod 187$

$= 77$

if $b_2 = 1$ 'N'

$c = 2$ $f = 77$

for $i = 1$

$C = 4$

$f = (77 \times 77) \bmod 187$

$= 132$

if $b_1 = 1$ Y

$c = C + 1 = 5$

$f = (132 \times 88) \bmod 187 = 22$

$c = 5 \quad f = 22$

for $i = 0$

$c = 10$

$f = (22 \times 22) \bmod 187$

$= 110$

if $b_0 = 1$ Y

$c = 11$

$f = (110 \times 88) \bmod 187$

$\boxed{f = 143}$

c is nothing but b value i.e. $88^{11} \bmod 187$

Efficient operation using the public key

- The choice of e is made such that the speed is increased
- Popular choice 3 and 17, as there are only 2 1's
- But small e is vulnerable

15-4-2021 The Security of RSA

Most happening Attacks

1. Brute Force Attack
2. Mathematical Attack
3. Timing Attack - Constant Exponentiation time, Random delay, Blinding
4. Hardware-fault-based attack
5. Chosen Cipher text Attack and

Diagram Optimal Asymmetric encryption padding