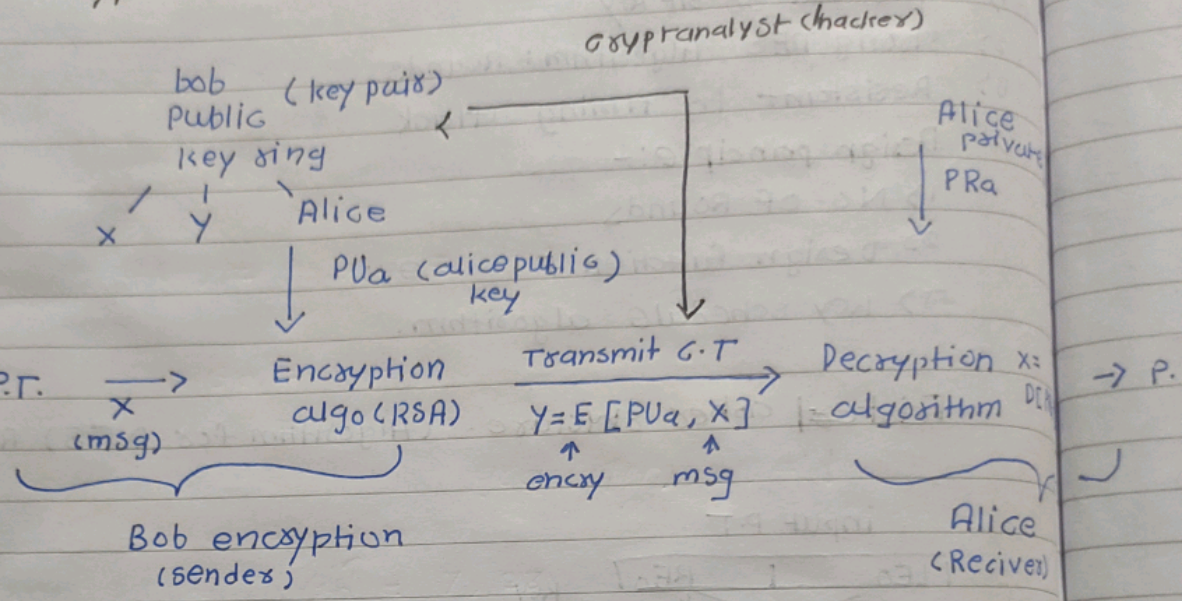
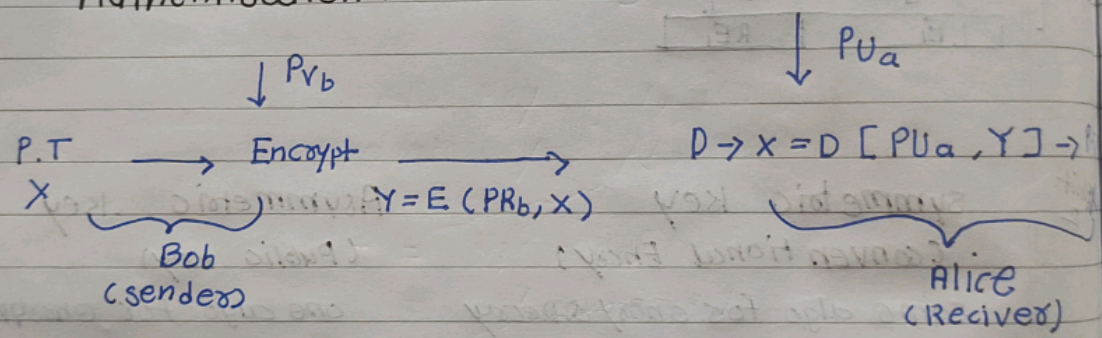
Unit:-2 Principle's of public key cryptosystems.

Encryption with public key (secrecy)



Authentication :-



RSA Algorithm :

1) Publickey cryptography

Problem

MSE 2)

Encryption :- $C = M^e \bmod n$ (C.T, Msg, encryp, sender) $M = C^d \bmod n$ (decryptn, Reciver)

1) select 2 prime no P & q resp. $P \neq q$
2) $n = P * q$
3) $\phi(n) = (P-1)(q-1)$
4) $ed = 1 + K\phi(n)$ (start K=0)

Calculate e, d key pair {e, n} (public) sender
{d, n} (private) Reciv

Analysis of SIP:

Lexical Rules:-

RSA algorithm RSA is a block cipher in which the P.T. & C.T are represented as integers both 0 and n-1 for some value of n Larger msg broke down into number of blocks. each block would then be represented by an integer

$ed = 1 + k\phi(n)$

select e (integer)
calculate d

$\gcd(\phi(n), e) = 1 \; ; \; 1 < e < \phi(n)$
$d = e^{-1} \pmod{\phi(n)}$

eg :-

Value of P = 3, q = 5, M = 4 (P.T)

P = 3, q = 5

$n = P \times q = 3 \times 5 = 15$

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

For $k = 0, k = 1$

$ed = 1 + k\phi(n)$

$= 1 + 1.8$

$ed = 9$

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

Suppose $e = 3, d = 3$

Public key = {3, 15}
Private key = {3, 15}

Now Cipher text $C = M^e \bmod n$

$= 4^3 \bmod 15$

$= 64 \bmod 15$

$= 4$ ~~26~~ (Remainder)

Plain text

$M = C^d \bmod n$

$= 4^3$

$M = 4$

$64 \bmod 15 \Rightarrow$ Ans $= 4 \Rightarrow$ Ans $\times 15$

4.0077

2) ~~P = 13, q = 17~~ P = 17, q = 11 M = 88

$n = P \times q$

$= 17 \times 11$

$n = 187$

$\phi(n) = 16 \times 10 = 160$

$ed = 1 + 160$

$= 161$

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

$\gcd(160, e) = 1$

$ed = 7, 23$

$e = 7, d = 23$

public key $\{7, 160\}$

private key $\{23, 160\}$

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

$= 88^7 \bmod 187$

$C.T = 11$

P = 3, q = 11, M = 5

$n = P \times q$

$= 11 \times 3 \Rightarrow 33$

$\phi(n) = 10 \times 2 = 20$

$ed = 1 + 20$

$= 21$

$e = 3$

$d = 7$

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

$= 5^3 \bmod 33$

$= 26$

The purpose of Piffie-Hellman algorithm is to enable two users to securely exchange a key that can be used for subsequent encryption of msg.

Diffie-Hellmen key exchange Procedure:- to achive asymmetric to exchange key beth two (S & R) encryption

Alice q prime number (consider)

α $\alpha < q$ and α is primitive root of

User key Generation

select private X_A $X_A < q$

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

User B key Generation.

X_B $X_B < q$

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

calculate of secret key by User A

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

for User B

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

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

$K = (\alpha^{X_B} \bmod q)^{X_A} \bmod q$

$K = (\alpha^{X_B})^{X_A} \bmod q$

$K = (\alpha^{X_B X_A} \bmod q)$

$K = (\alpha^{X_A})^{X_B} \bmod q$

$K = (\alpha^{X_A} \bmod q)^{X_B} \bmod q$

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

Primitive Root:- eg: 5 and 7 5 is primitive of 7

3 " " 7

let P as a prime number

then a is primitive root of P if the powers a modulo P all integers from 1 to P-1 in

Some permutation $\underline{P-1}$

$a \bmod p,\ a^2 \bmod p,\ \dots,\ a^{p-1} \bmod p$

eg: $p = 7$ then primitive root is 3 cause power of $3^{i+1} \bmod 7$ generates all the integers from 1 $(i = 0)$

$3 \pmod 7 = 3 = 3^1$

$3^2 = 9 \pmod 7 = 2$

$3^3 = 27 \pmod 7 = 6$

$3^4 = 81 \pmod 7 = 4$

$3^5 = 243 \pmod 7 = 5$

$3^6 = 729 \pmod 7 = 1$

$P-1 = 7-1 = 6$ (upto)

example :-

IMP 1) $q = 23$

$\alpha = 5$ primitive root of q.

Alice selects private key $X_A = 6$

alice computes

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

$Y_A = 5^6 \bmod 23$

$Y_A = 8$ (alice public key)

Bob private key $X_B = 15$

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

$= 5^{15} \bmod 23$

$= 19$ (bob public key)

alice Y_A to bob send Y_B to alice

Alice computes key $K = (Y_B)^{X_A} \bmod q$

$= (19)^6 \bmod 23$

$K = 2$

Bob computes key

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

$= (8)^{15} \bmod 23$

$K = 2$

2) $q = 19$, $\alpha = 10$, $X_A = 7$, $X_B = 8$

Given $X_A = 7$

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

$= 10^7 \bmod 19$

$= 15$

$10^7 \% 19 = \text{Ans} \times q + \text{Ans}$

$13^{26} \bmod 5 = 12^{23}$

$X_B = 8$

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

$= 10^8 \bmod 19$

$= 17$

Y_A to bob send Y_B to alice

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

$= (17)^7 \bmod 19$

$= 5$

alice calculate shared secrete key $K_A = (Y_A)^{X_B} \bmod q$

$= (15)^8 \bmod 19$

$= 5$

IMP Message Authentication : Hash function (not use key)
Use For Data integrity

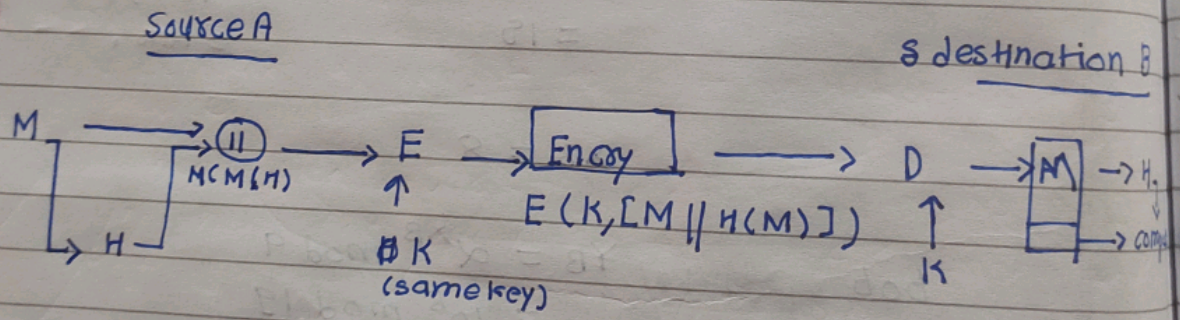
L bits Msg M → Hash function H → hash value $h = H(M)$

Hash fun^n use for Data integrity.

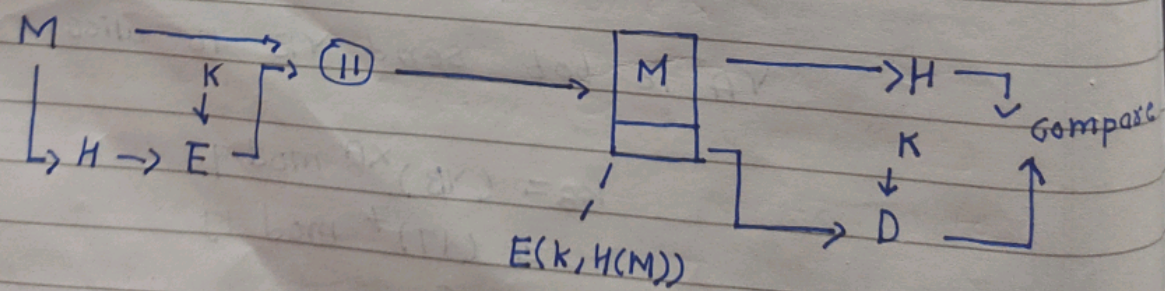
h value arrive at Reciver → Hash fun^n → h it check this h value and previous h value if same data integrity should be there.

How Authentication is achive (way's)

A)



B)



MSg Authentication (MAC) Msg Authentication code (use key)

- uses a shared secret key to generate a MAC (cryptographic checksum)
- MAC append to the MSg
- A → B uses same secreate key

calculate the MAC

$$MAC = C(K, M)$$

- A sends (MAC+M) → B
- B performs the same (M+MAC) using the secrete key it generate New MAC'
- Recived MAC compared with new MAC' if same then data is recived successfully.

eg:

Msg - Helloy , K

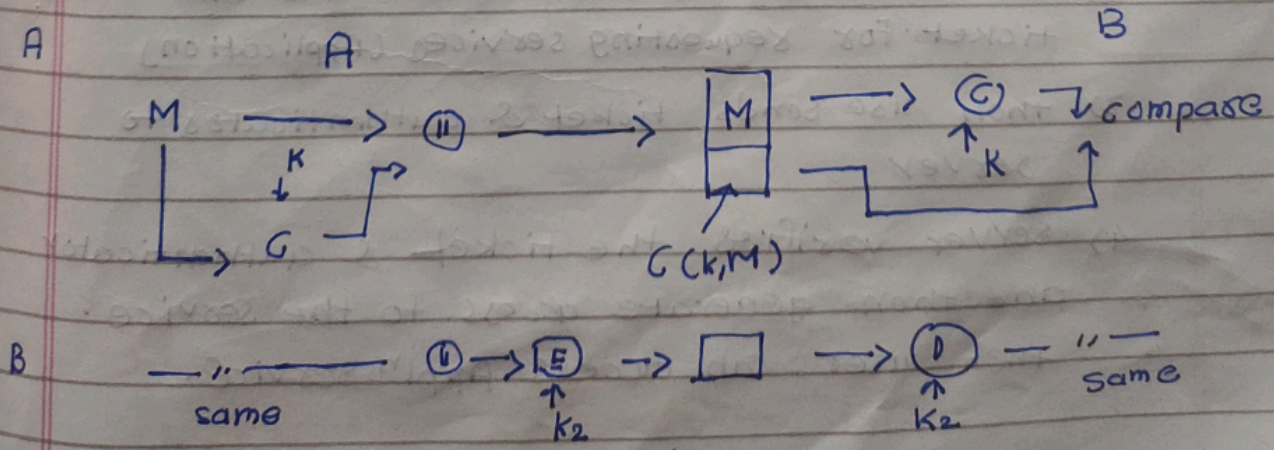
MAC = C(K, Hello)

= pqrst

MAC = C = Hello + pqrst

MSg ↕ compare.

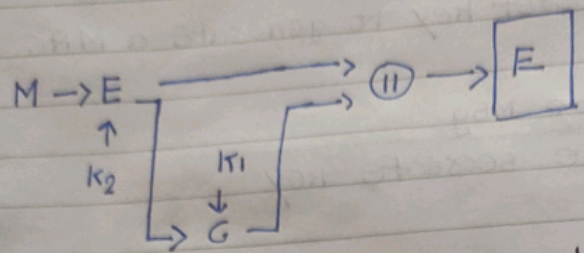
MAC' = (K, Hello) = pqrst



authentication tied to plain text

Unit

Authentication tied with cipher text



Possible approaches to attacking the RSA algorithm

1) Brute force
2) Mathematical attack
3) Timing attacks
4) H/w fault-based attacks
5) chosen ciphertext attacks.

~~Authentication key~~.

→ kerberos

1. user login and request to host for ticket granting service

Authentication server (AC) verfies user access in DB and then send Encrypted response granting ticket and session key user Decrypted using user key

2) then user send ticket to ticket granting server (TGS) the ticket contain username & N/w address
Now TGS server verfies ticket and then create ticket for requesting services (Application)

3) then use sends ticket & authenticator to server

4) server verifies the ticket & authenticator and then generate access to the service. then user can access Appln service.