UNIT-3

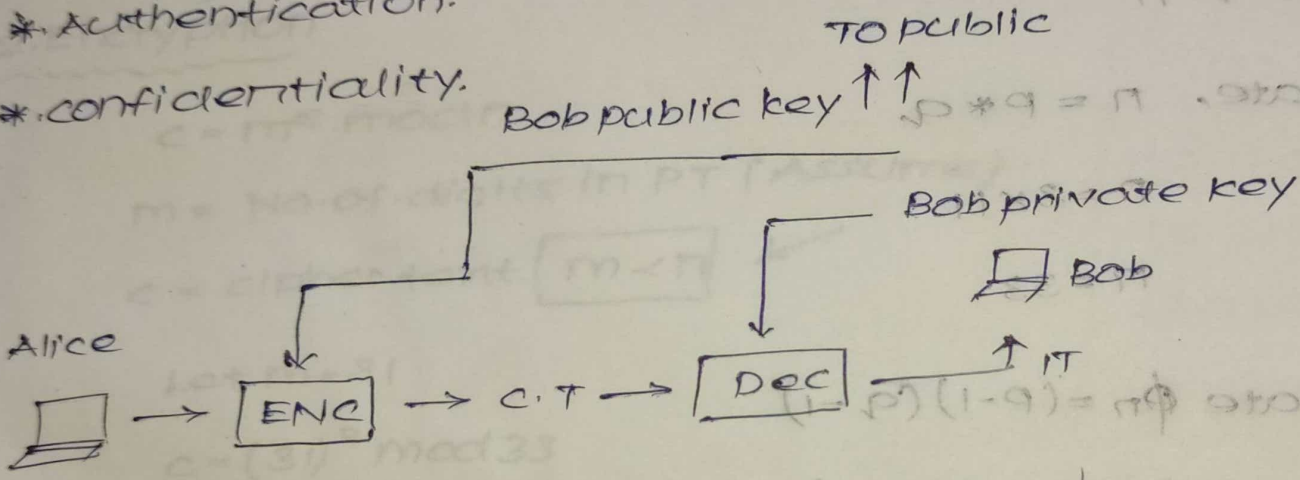
Public key cryptography

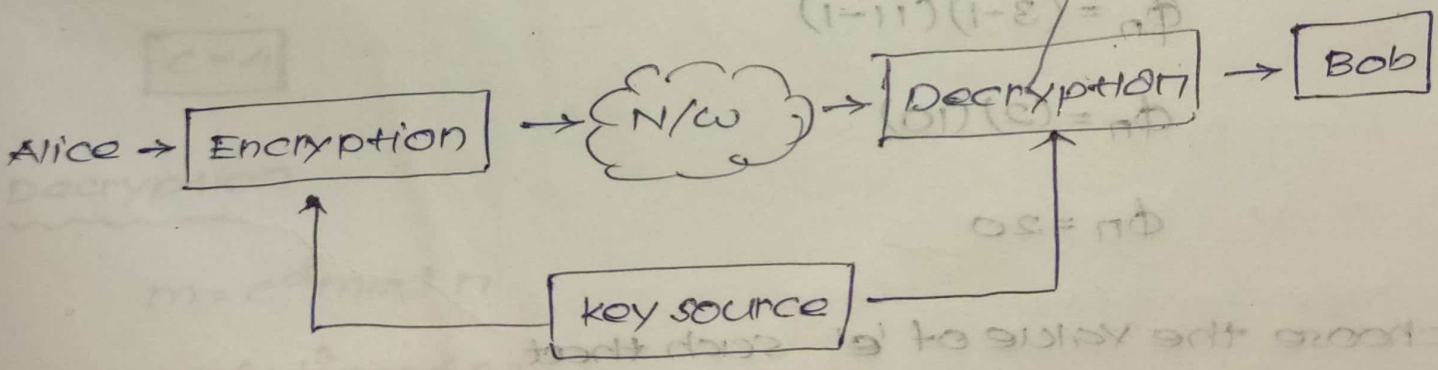
Symmetric key → 1 key same

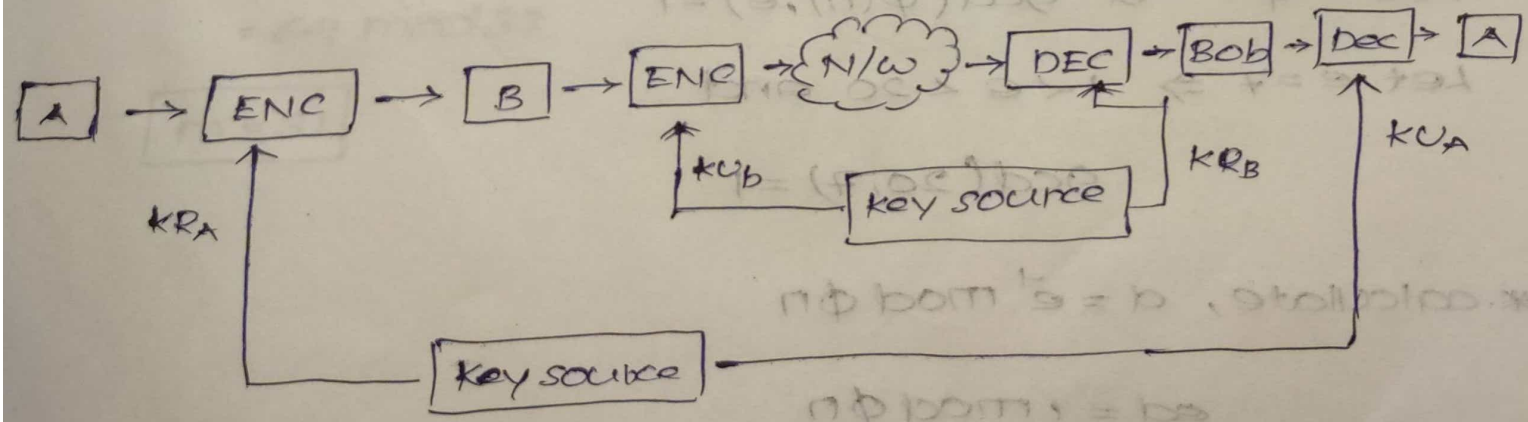
Asymmetric key → 2 different keys

2 Difficulties

* KDC
* Digital signature
* properties
* Authentication.
* confidentiality.







* RS Algorithm

(Rivest - Shamir - Adleman)

3 steps : 1) Key generation

2) Encryption

3) Decryption.

1) Key Generation

* select two large numbers p and q for more security

p=3, q=11

* calculate, $n = p * q$

$n = 3 \times 11$

$n = 33$

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

$\phi_n = (3-1)(11-1)$

$\phi_n = (2)(10)$

$\phi n = 20$

* choose the value of 'e' such that

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

Let $e = 7 \Rightarrow 1 < e < 20$ and

$gcd(20, 7) = 1$

* calculate, $d = e^{-1} \bmod \phi n$

$ed = 1 \bmod \phi n$

* public key = {e, n}

= {7, 33}

* private key = {d, n}

= {3, 33}

2. Encryption

$c = m^e \bmod n$

m = No. of digits in PT (Assume)

c = cipher text $\boxed{m < n}$

Let m = 31

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

$\boxed{c = 4}$

3) Decryption

$m = c^d \bmod n$

$= (4)^3 \bmod 33$

$= 64 \bmod 33$

$\boxed{m = 31}$

* Euler's Totient function (Phi fln)

* Denoted by symbol $\phi(n)$

condition:

$\phi(n)$ = Number of positive numbers less than 'n' that is negative prime to n.

Ex: Find $\phi(5)$

Sol: $n = 5$.

Numbers less than 5 are 1, 2, 3, 4.

Relatively prime (1, 5) (2, 5) (3, 5) (4, 5)

GCD	
GCD(1,5)=1	✓
GCD(2,5)=1	✓
GCD(3,5)=1	✓
GCD(4,5)=1	✓

$\phi(5) = 4$.

Ex: Find $\phi(11)$

Sol: $n = 11$

Number less than 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Respectively prime (1, 11) (2, 11) (3, 11) (4, 11) (5, 11) (6, 11) (7, 11) (8, 11) (9, 11), (10, 11).

$\phi(11) = 10$.

*. Fermat's little Theorem :

$P = 13$ and $a = 11$

$11^{13-1} = 1 \pmod{13}$

$11^{12} = 1 \pmod{13}$

* Euler's Theorem

For every positive integer 'a' & 'n' which is said to be relatively prime then $\phi(n) \equiv 1 \bmod n$

Ex: prove euler's theorem hold true for $a = 3$ & $n = 10$

$GCD(3,10) = 1$

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

$3^{\phi(10)} \equiv 1 \bmod 10$

$3^4 \equiv 1 \bmod 10$

$81 \equiv 1$

TO

$1 \equiv 1$

$\phi(n) = 10$

$= 2 \times 5$

$= (2-1)(5-1)$

Diffie Hellman key Exchange

*. Not an encryption / decryption algorithm.

* use to exchange keys between sender and Receiver.

*. A symmetric key cryptography

procedure

1. consider a prime number q

let $q = 7$

2. select α such that $\alpha < q$ and α is primitive root

of 9

Primitive root

$\alpha^1 \bmod 9$

$\alpha^2 \bmod 9$

$\alpha^3 \bmod 9$

$\alpha^{9-1} \bmod 9$

Let $\alpha = 3$

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

$\alpha = 5$

$5^1 \bmod 7 = 5$

$5^2 \bmod 7 = 4$

$5^3 \bmod 7 = 6$

$5^4 \bmod 7 = 2$

$5^5 \bmod 7 = 3$

$5^6 \bmod 7 = 1.$

3. Assume X_A (Private key of A)

X - Private

Y - Public

$\boxed{X_A < 9}$ $\quad Y_A = \alpha^{X_A} \bmod 9$

$X_A = 3$

$Y_A = (5)^3 \bmod 7$

$\boxed{Y_A = 6}$

4. Assume X_B where $\boxed{X_B < 9}$

$Y_B = \alpha^{X_B} \bmod 9$

$= (5)^4 \bmod 7$

$= 2$

5. calculate the secret key.

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

$= (2)^3 \bmod 9$

$= 1$

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

$= (6)^4 \bmod 9$

$= 1$

$\boxed{K_1 = K_2}$

UNIT-4

Authentication and Hash functions

Authentication function.

Authentication:

Verifying the identify of the user i.e. user is a correct person or not.

* Authentication is generated by Authentication function.

There are three types of Authentication function.

1. Message Encryption.
2. Message Authentication code (MAC)
3. Hash function.

1. Message Encryption

* converting Plane text to cipher text.

2. MAC:

C(M, K) = O/P (fixed length function)

C = Authentication function

M = Message.

K = key

O/P = MAC code.

3. Hash function:

* It is similar to MAC. Instead of K we use Hash

$H(M) \Rightarrow$ o/p (fixed length code)

hash code - H.

*. Message Authentication code (MAC):

* Symmetric key cryptography use

↓

same key.

Working of MAC:

Sender side. M ↓ C.T ← symmetric key

Receiver side M ↓ H_2 C T ← key.

$H_1 = H_2$

*. MD5 (Message Digest Algorithm)

*. It is developed by Rivest.

*. Fast and produces 128 Bit message Digest.

*. Message digest Breaking the message into number of pads.

*. Working of MD5

1) Padding

original message + padding

such that total length is less than 64 bit exact multiple of 512.

Ex: 1000 Bits + padding

512 × 1 = 512 bit - 64 = 448

512 × 2 = 1024 bits - 64 = 968

512 × 3 = 1536 bits - 64 = 1472 pads = 472.

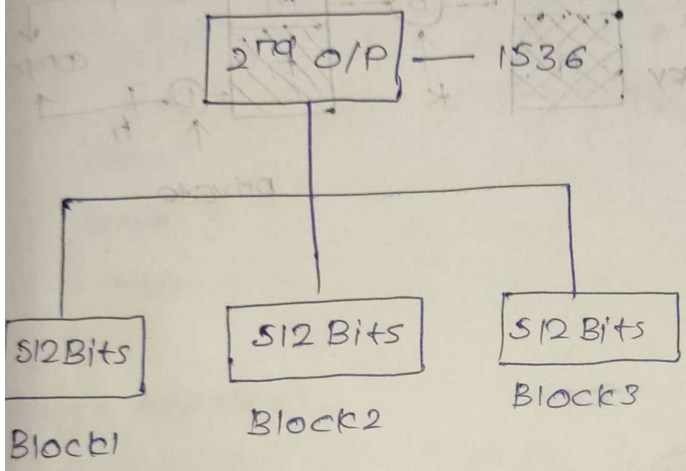
2) Append

= 1472 + 64

= 1536

3) Dividing each 512 bits

512 × 3 = 1536.



4) Initialising (4 chaining variables)

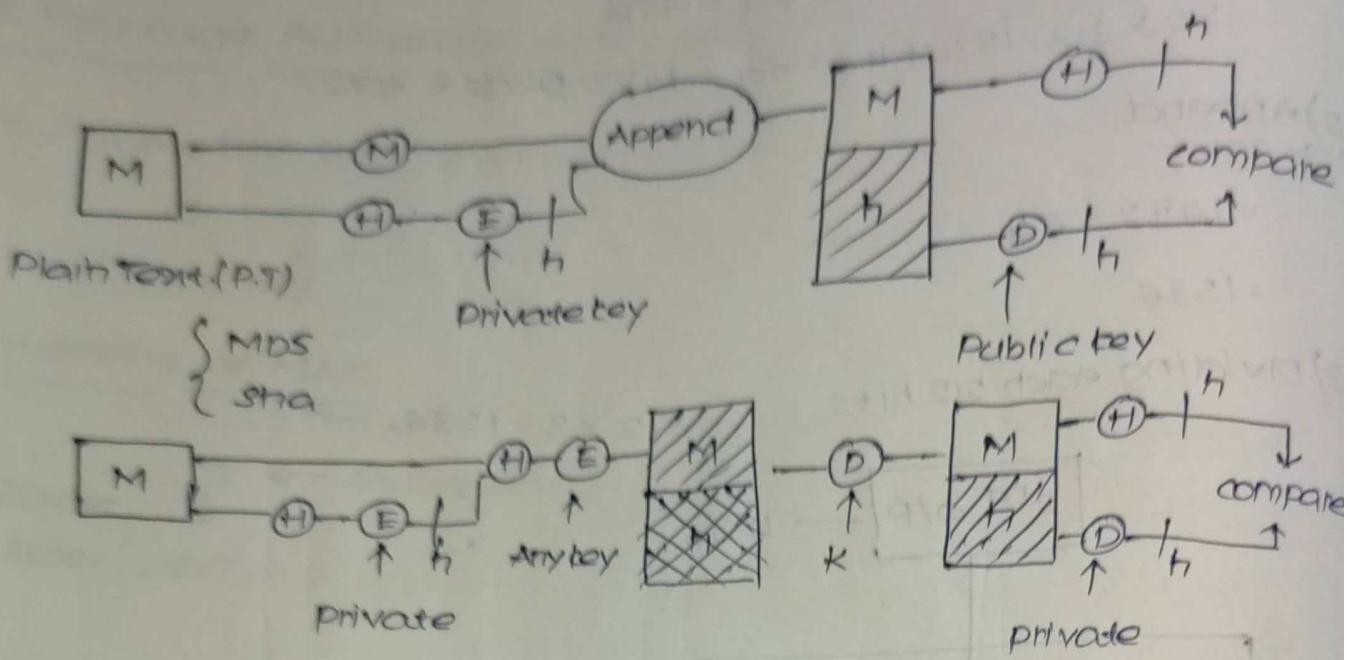
Each variable = 32 bits

A, B, C, D → Values Predefined.

5) copy (4) chaining variables into some corresponding variables

A = a, B = b, C = c, D = d.

*. Hash function



*. Sha Algorithm

o/p - 160

A, B, C, D, E

1. Padding.
2. Append.
3. Dividing 512 bit
4. process the variables - Buffer
5. o/p in Message Digest

*. HMAC

HASH + MAC

1. Compute 8 bits.
2. Append. 8 || M (P.T)
3. perform Hashing function.

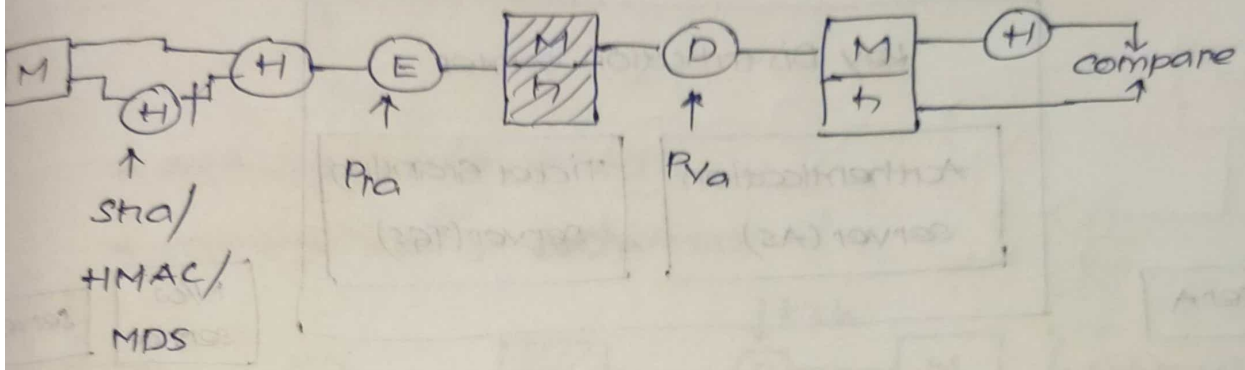
Digital signature

* sender - Encryption.
* Receiver - Decryption.

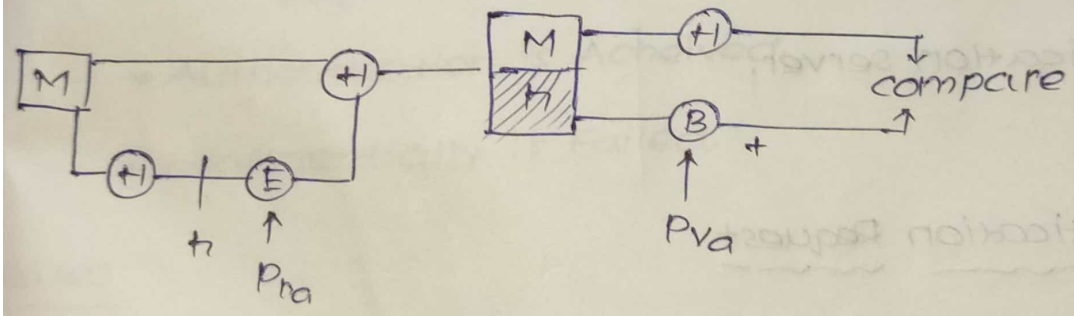
2. keys ⇒ Asymmetric key.

* Encryption we use private key is called digital signature

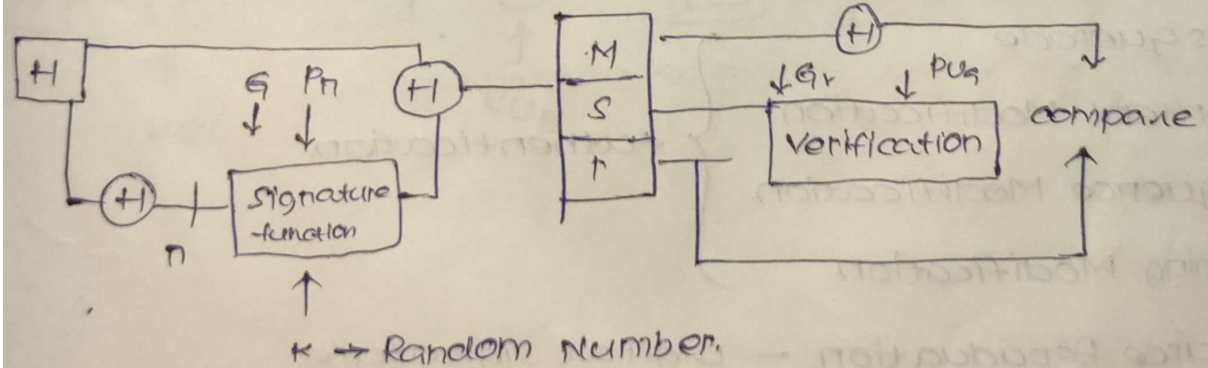
* same set of keys used either A or B



1) RSA Approach

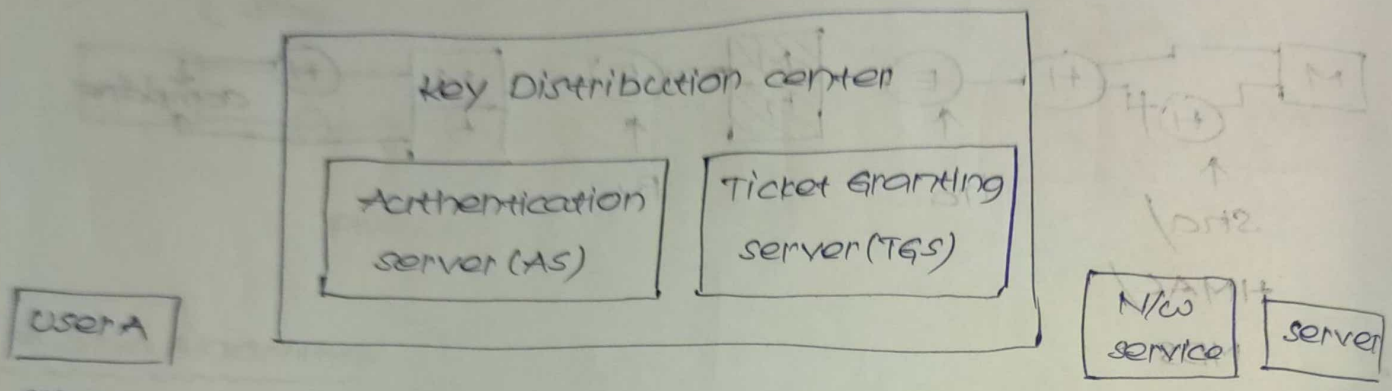


2) Digital signature standard.



*. Authentication protocol

* It is a network authentication protocol it is follows direct and server Architecture
* It uses a symmetric key
* It request the third party key. (KDC)



*. Two different Tickets.

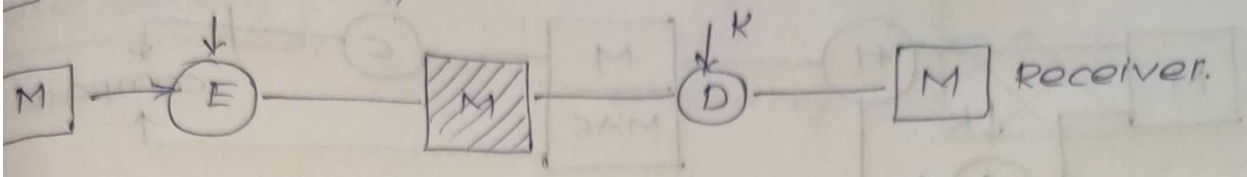
1. Authentication server.
2. TGS.

*. Authentication Request

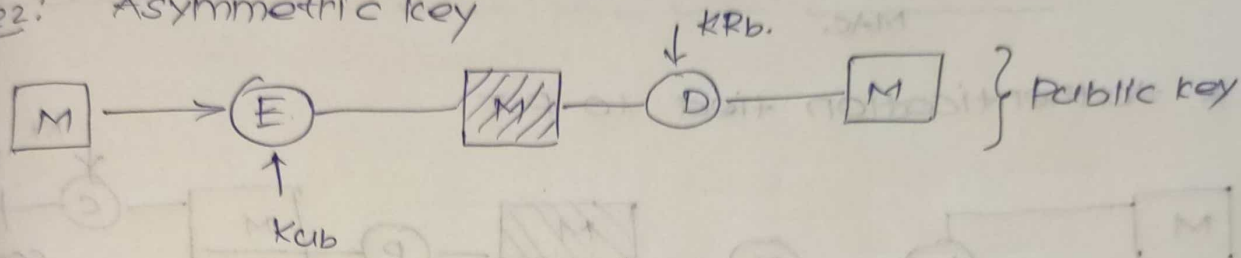
1. Disclosure
2. Traffic Analysis. } confidentiality
3. Masquerade
4. content Modification.
5. sequence Modification.
6. Timing Modification } Authentication.
7. source Repudiation. — Digital signature.

Message Encryption

case1: Symmetric key

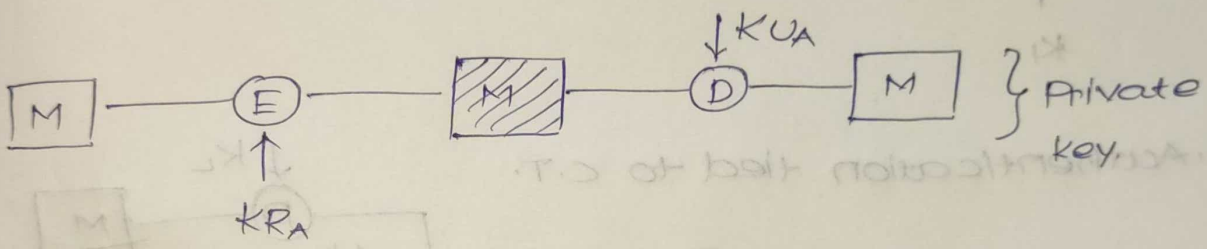


case2: Asymmetric key



*. Authentication failed

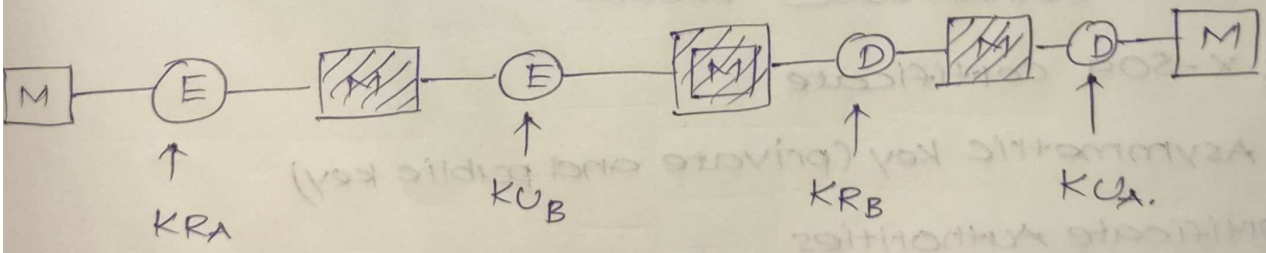
*. confidentially acheived.



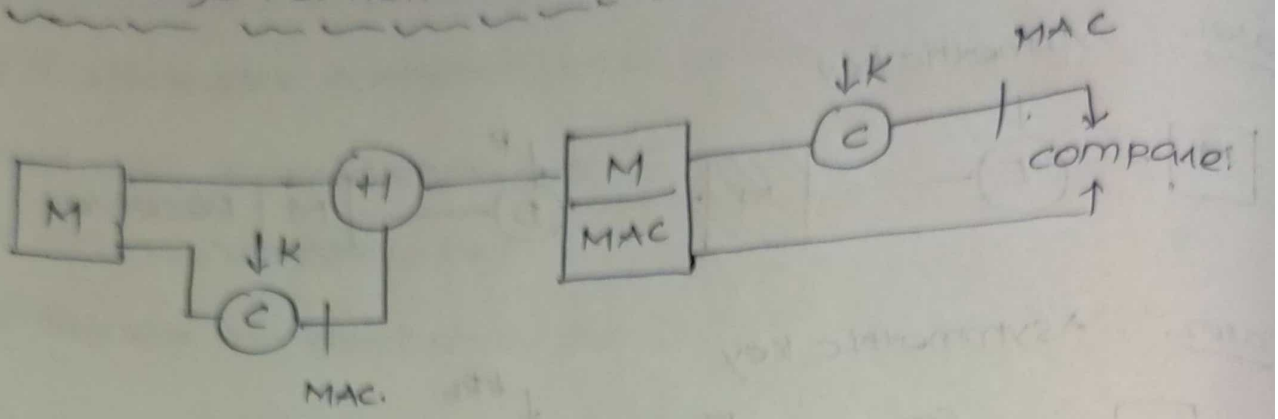
*. Authentication is Acheived.

*. confidentially is Failed.

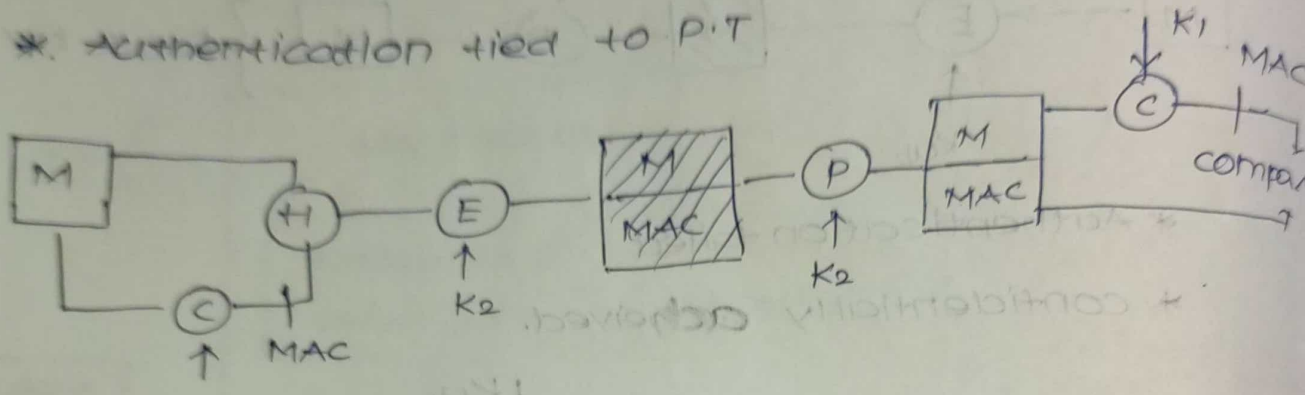
case3:



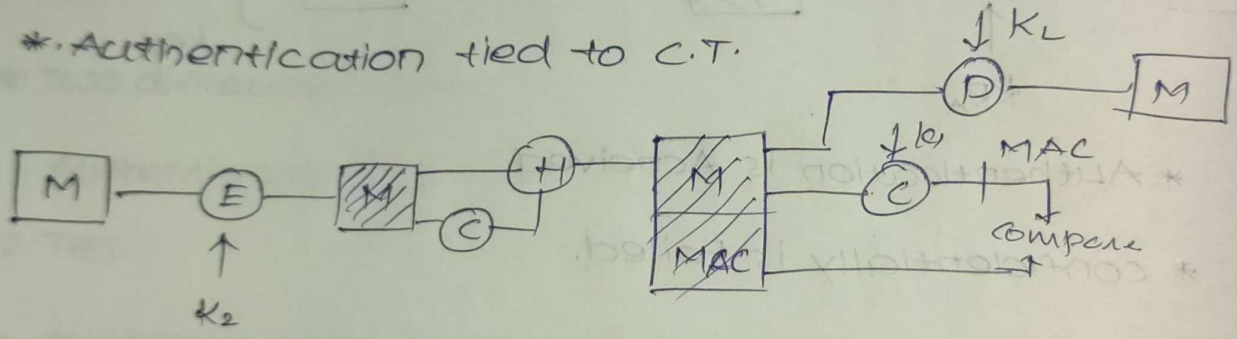
*. Message Authentication code (MAC):



*. Authentication tied to P.T



*. Authentication tied to C.T.



*. X-509 Authentication service

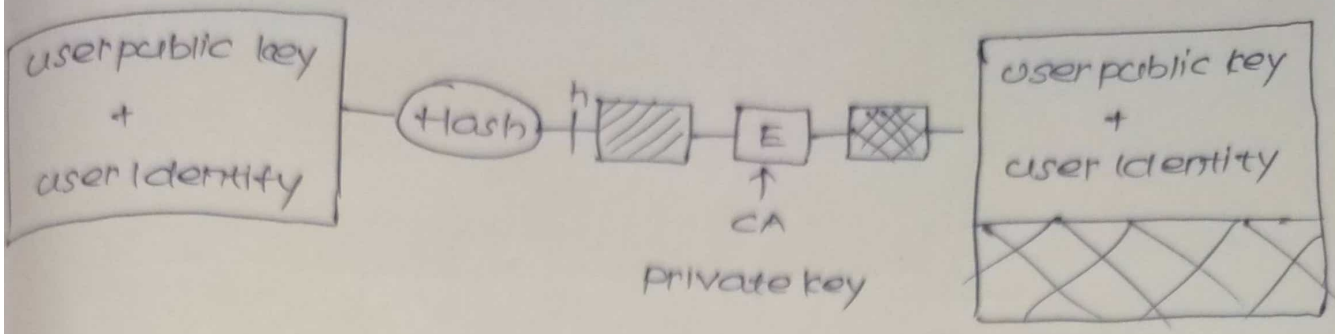
*. X-509 certificate

*. Asymmetric key (private and public key) certificate Authorities

*. Trusted 3rd party

*. CA Generator signature

*. It is stored in x-509 certificate directories.



certificate format / Fields of X-509 certificate