Cryptography

Components :—

① Integrity ② Confidentiality ③ Non-repudiation ④ Availability
⑤ Access control ⑥ Authentication.

Integrity :— Message shouldn't modified in b/w sender & receiver.

Attacks :—

① Passive Attack
② Active Attack } Diff of Active & Passive Attack

Security Attacks

a) Interruption b) Interception c) Modification d) Febrication

Passive Attack :—

a) Release of message content
b) Traffic analysis.

Active Attack :—

a) Masquarade b) Replus c) Modification of the sequence
d) Deny of service.

Cryptography :—

To hide the actual message / context.

Category of Algo :—

① Symmetric Key Cryptography : both side the Key is same
② Assymmetric Key cryptography : different Key used.

a) Plain Text :— Before sending the message / before sending to receiver.

b) Cipher Text :—

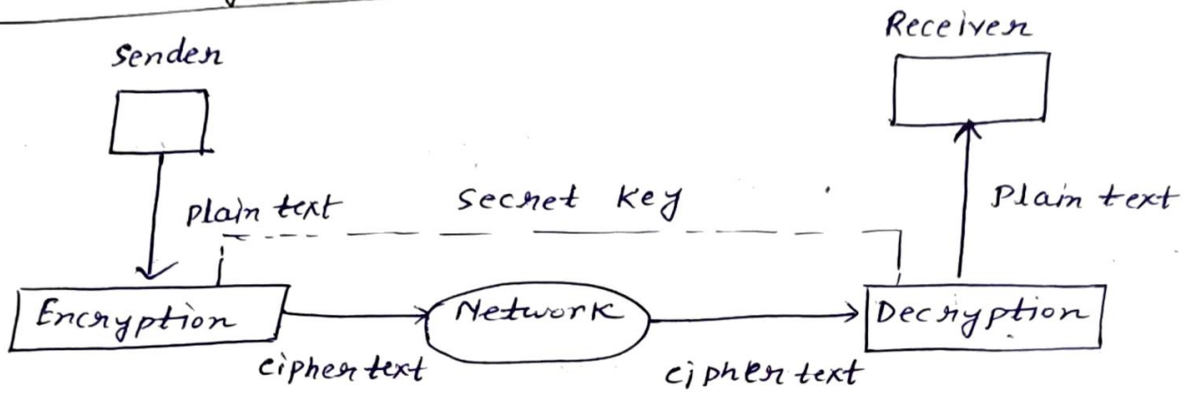
- Crypto analysis
- Cryptography } Concept

16.02.24

Cryptographic Algorithm :—

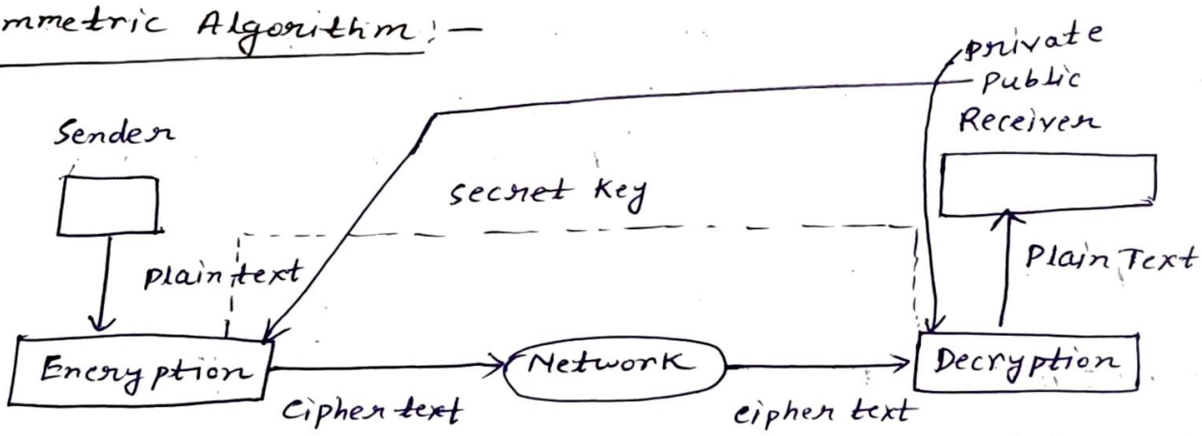
1) Symmetric Algorithm / Private Key ex DES (Algo)
2) Assymmetric Algorithm / Public Key ex. RSA (Algo)

Symmetric Algorithm :—



- Write a short note on → Private Key / Public Key etc.
- If there are 'n' number of users then there are total $^nC_2$ no of secret keys.

Assymmetric Algorithm :—



Symmetric Algo :—

Same key for encryption & decryption.

Assymmetric Algo :—

Encryption done by public key,
Decryption done by receiver secret / Private Key.

Cipher

- Cipher (Traditional)
  - Substitution Cipher
    - Mono-Alphabetic
    - Poly-alphabetic
  - Transpositional Cipher (only position will change)

Mono-Alphabetic Cipher:- one to one mapping relation b/w plain text & cipher

P → A L I A H Key = 2

C → C N K C J (A → C)
Ⓟ Ⓒ

Caesar Cipher (one type of mono alphabetic cipher)

Here the key value is fixed as 3

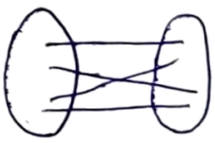
(A → D)
Ⓟ Ⓒ

Problem of Monoalphabetic Cipher:-

As it is very simple user can break the code easily and get to know about the plain text or message easily.

If 'A' is used in the cipher as 10 times and replaced by e then we can easily got the code.

Polyalphabetic Cipher (one to many)



P → A L I A H Key = 2

C → E H J D K

- Vigenere Cipher

P → B R I C K

C →

P → A B D D X Y

C → E F H

A – Z
1 – 26

D – M
D – V

Position of the text / → mode

Advantage:- It is difficult to break the code.

Transportional Cipher (only the position will change)

	1	2	3	4	5	6
P →	S	U	N	D	A	Y

(Row wise or column wise)

Y	A	
X	Y	- - -
D	Z	- - -

C → Y A U

Y X D A D Z

HE is a GOOD BOY
HE GOES UNIVERSITY ALL DAY

HH EE IG So . . . . .

Advantage :-

- Little bit complex
- Much more secure than substitutional.

Suggestion

1) Definition of security, aspect of security
2) Different types of pattern. Diff types of attack
3) Diff types of algorithm
4) DS algorithm (Diagram), RSA Algo * Traditional, crypto analysis ~~algorithm~~
5) Cryptographical Algo. How to calculate diff types of algo.
6) Message Digest
7) Davy-Hellman protocol. * Protocols .. What is the use of protocol
   * Numerical protocol.
8) Man in the middle attack
9) Security protocol on different layer (In Details)
10) Frame Protocols (Firewalls, different) * Diff types of firewall
11) VPN, DMZ Network, SJ protocols, authentication mechanism
12) SMTP, POPS protocol., STP
13) Image Security protocols, Gmail protocol

6.03.24

Polyalphabetic Cipher

Transpozitional "

Monoalphabetic :-

Ex :-

W	A	S	I	M	A
↓	↓	↓	↓	↓	↓
Y	C	U	K	O	C

Key : 2

Polyalphabetic :-

W	A	S	I	M	A
↓					↓
X	B	T	U	Z	D

one to many

1) Vigenere Cipher :-

$$C_i = \left(P_i + K_{i \bmod m}\right) \bmod 26$$

Ex :- Key value = XYZ PT = WASIMA

Key	X	Y	Z	X	Y	Z	X
PT	W	A	S	I	M	A	A
CT	T	Y	R	F	K	Z	X

24+0

W X

22 + 23 = 45

45 mod 26

= 19 = T

Transpozitional Cipher :-

PT = TODAY IS WEDNESDAY

Key = 53214

CT = ?

1	2	3	4	5
T	O	D	A	Y
I	S	X	X	X
W	E	D	N	E
S	D	A	Y	X

Blank Box → X

Now

5	3	2	1	4
Y	D	O	T	A
X	X	S	I	X
E	D	E	W	N
X	A	D	S	Y

CT = YXEXDXDAOSEDTIWS AXNY

Block Cipher 64 bit
Stream Cipher 8 bit

11010111
00010011

DES (Data Encryption Standard):-

64 bit plaintext

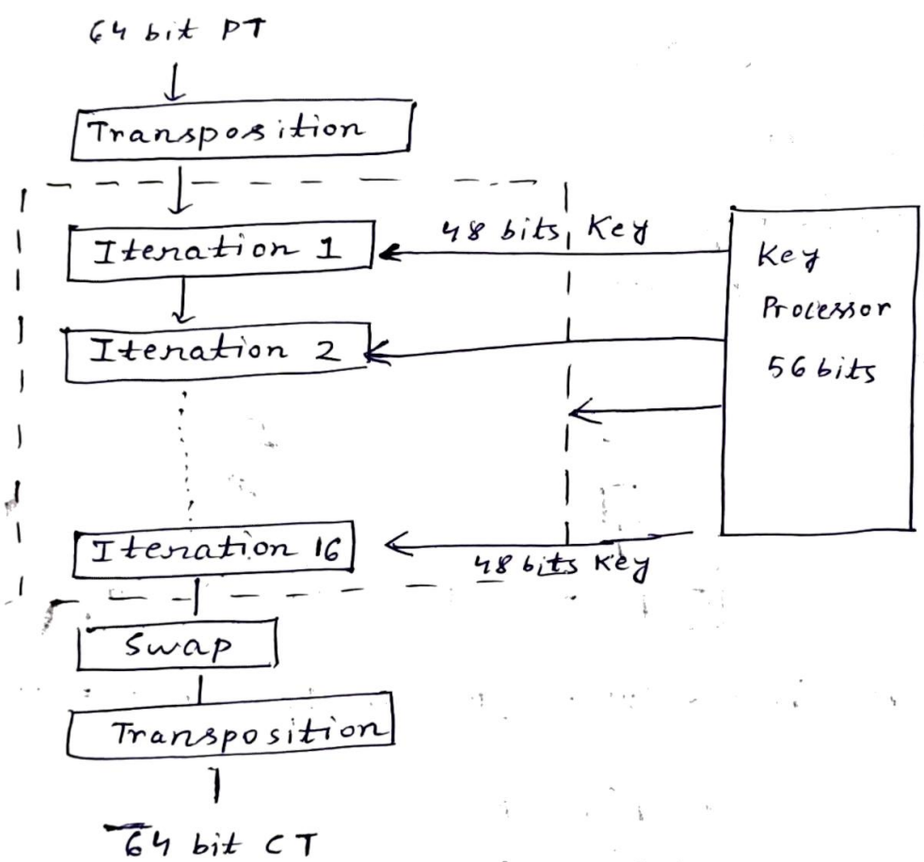
↓

Encryption ← 48 bit Key ← 56 bit Key Processor

↓

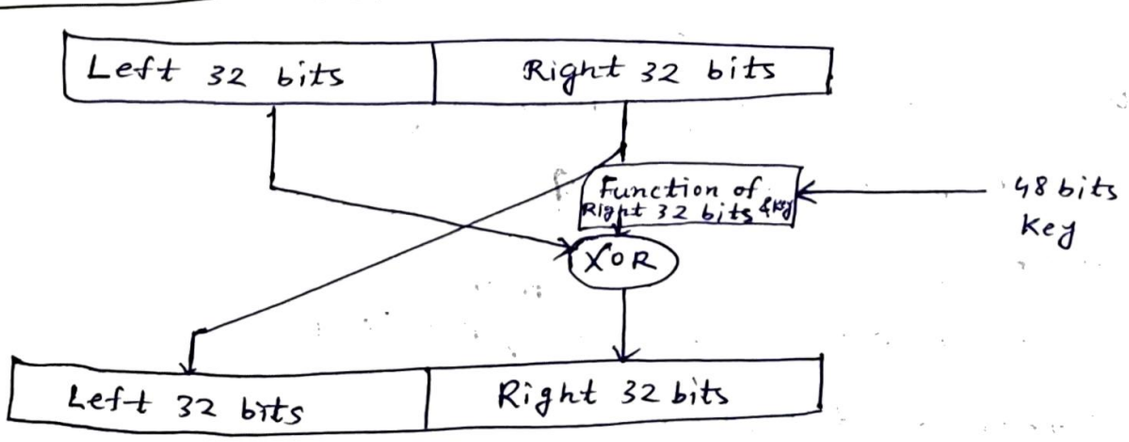
64bit cipher Text

General Structure of DES



Iterations:- 64 bits

XOR Gate

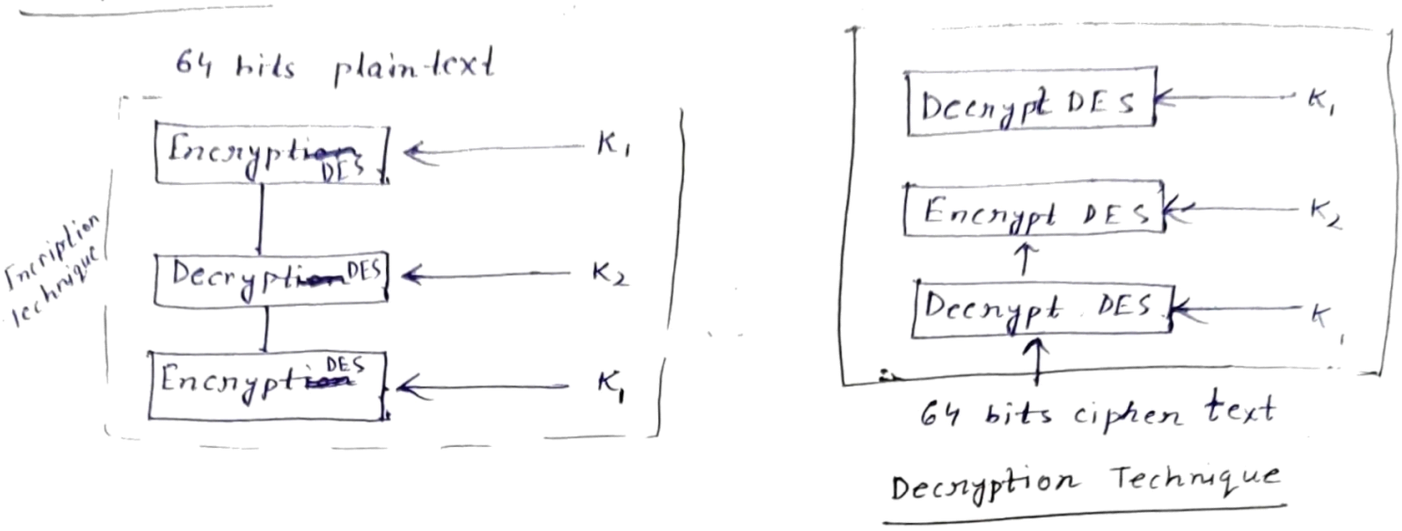


Size of Key value of DES Algo:—

" " " Process of DES — 56 bits

7.03.24

Tripple DES



Decryption Technique

RSA Public Key Cryptography algo

Symmetric → Private Key

Asymmetric → Public Key

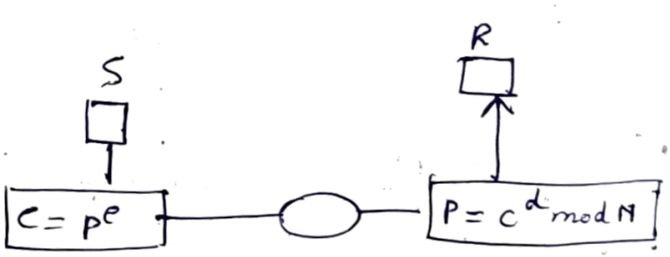
In this algorithm two Keys are used

Public Key = (N, e)

Private Key = (N, d)

$C = p^e \bmod N$

$P = c^d \bmod N$



Suppose the public key is $(N, e) = (119, 5)$. Private key $= (N, d) = (119, 77)$

$P = c^d \bmod N$

$= 43^{77} \bmod 119$

$= 8$

$c = p^e \bmod N$

$= p^5 \bmod 119$

$= 8^5 \bmod 119$

$= 43$

How we will choose Private Key & Public Key

1) Choose any two large number p & q

2) Calculate $N = P \times q$

3) Choose e such that e will be less than N and $(P-1)(q-1)$

4) Choose d such that $e \times d \bmod (P-1)(q-1)$

$P = 13, \quad q = 17$

$N = 13 \times 17 = 221$

$e \times d \bmod 221$

$e < N$

$(P-1)(q-1) = 12 \times 16 = 192$

Assignment

1) ~~Choose~~ Given two prime number $p = 19$ and $q = 23$. Try to find N, e, d

2) In RSA algo find d where $e = 17$ and $N = 187$.

~~Key aspe~~

13.03.24

Message Security :-

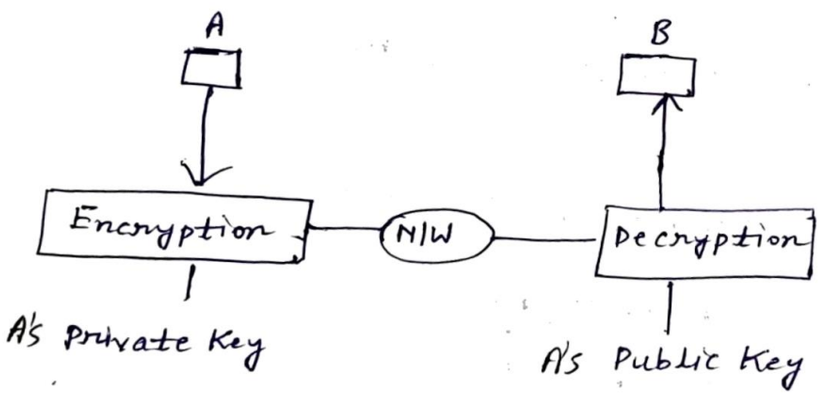
i) Privacy ii) Authentication iii) Integrity iv) Non Repudiation.

Digital Signature :-

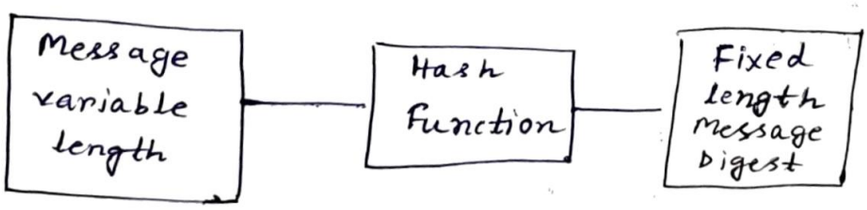
1) The digital signature does not provide privacy if there is a need for privacy another layer of encryption-decryption can applied.

2) Digital signature can provide integrity, authentication and non-repudiation.

3) In digital signature the private key is used for encryption and public key for decryption.



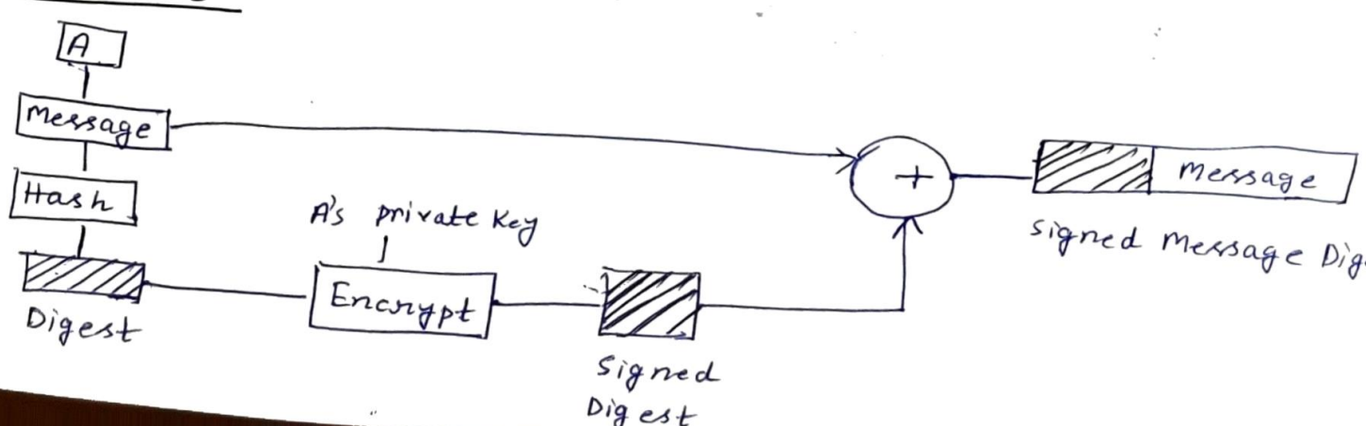
Message Digest



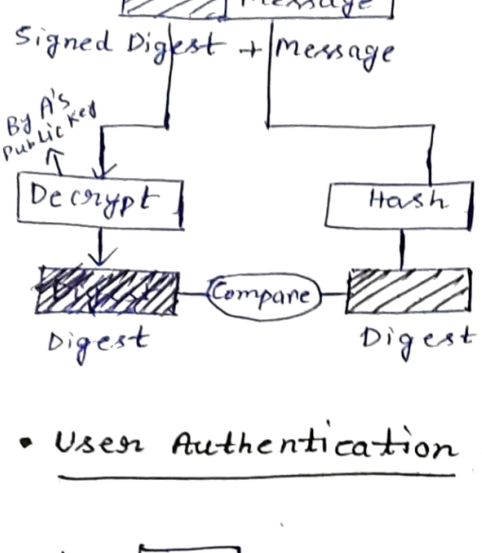
Hash function → MD5 → 120 bit digest
→ SHA1 → 160 " "

MD5 → Message Digest
SHF → Secure Hash Algorithm 1

Sender Side

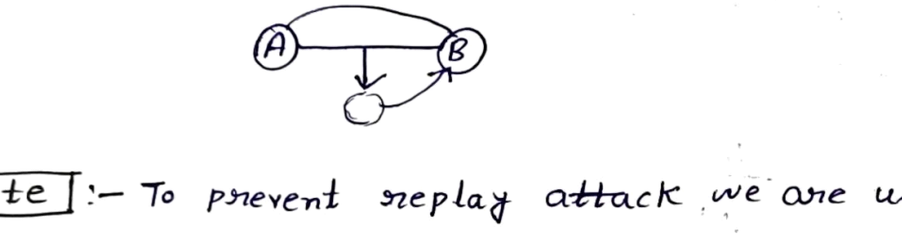


Receiver Site

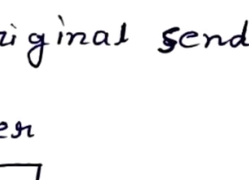


14.03.24

- **User Authentication :-**



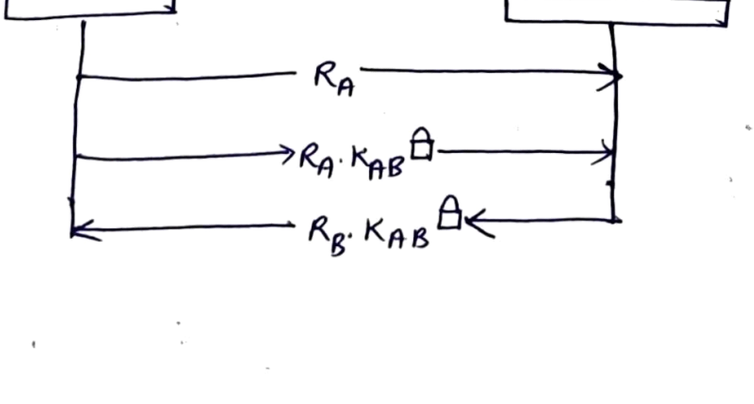
↳ Replay attack



Note :- To prevent replay attack we are using Nonce

2n Nonce :-

check the original sender, receiver and original

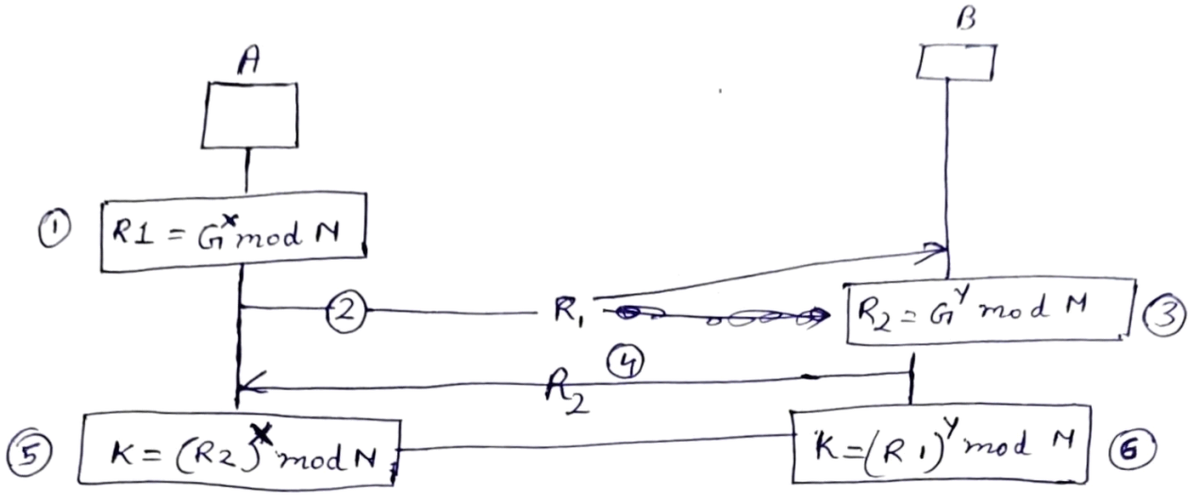


Symmetric Key Algo

n^2 problem

$\frac{n(n-1)}{2} = {}^{n}C_2$

Diffie Hellman ~~Problem~~ protocol (Key exchange protocol)



Symmetric key

$K = (R_2)^x \bmod N$

$= (G^y \bmod N)^x \bmod N$

$= G^{xy} \bmod N$

$K = (R_1)^y \bmod N$

$= (G^x \bmod N)^y \bmod N$

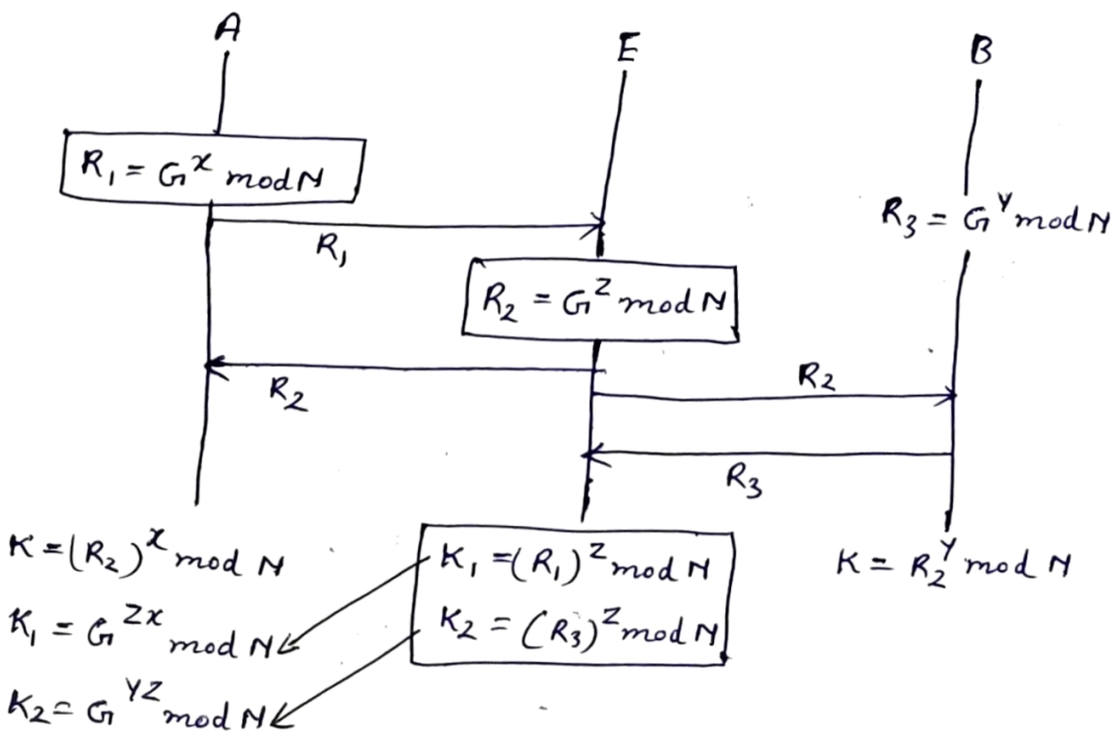
$= G^{xy} \bmod N$

G, N
Prime number

Man in the middle attack.

20.03.24

Man in the middle attack



Key Distribution Center (KDC algo) :-

Needham Schroeder Protocol

Oatway Rees Protocol.

Subdivision, purpose of KDC.

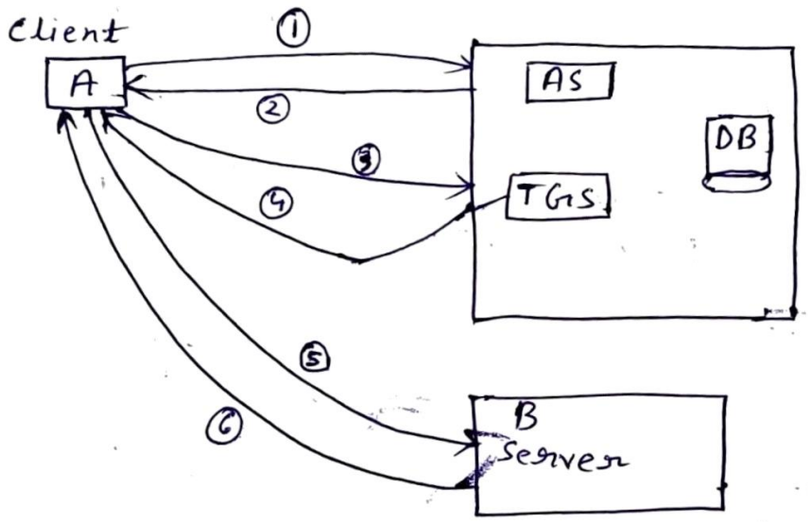
Kerberos (10/2 marks)

It has its own authentication, database

1) AS (Authentication Server)

2) Database

3) TGS (Ticket Granting Server)



Steps :-

1) Request Ticket for TGS

2) A TGS session key & ticket for TGS

3) Request ticket for B

4) A-B session key & ticket for B

5) Request Service

6) Provide service

TCP/IP
10/12

Security Layer Protocols

application layer

Transport "

Network "

Security Protocols :—

3-4-24

- IPSEC ——— AH
- IETF
- Signaling Protocol
  ~~Main~~ Establishes connection b/w two hosts

Modes

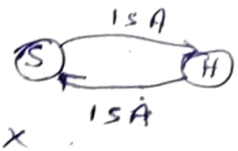
Transport Mode

Tunnel Mode

SA (Security Association)

Main Component of Security Association

SPE
Type of protocol
Source IP address
Security Parameter Index



Sec → Security

IP Header	The rest of Packet

IP Header	IP Security Header	The rest of Packet

Transport Mode

New IP Header	IP Sec Header	IP Header	The rest of Packet

Tunnel Mode

AH (Authentication Header) Protocol :-

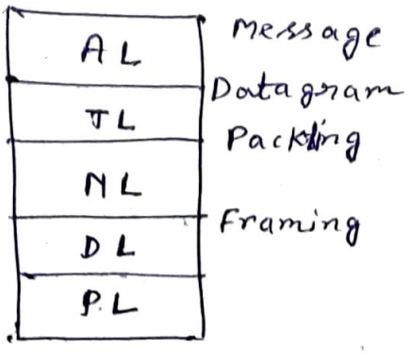
IP Header	AH	Rest of Packet	Padding

51

8 bits	8 bits	16 bits
Next Header	Payload length	Reserved bit
SPI (security, Parameter Index)		
Sequence Number		
Authentication Data (Digest) variable length		

- The data used in the calculation of Authentication data except those header in IP leader changing during transmission
- Type of the payload carried by the IP datagram.

- Transport layer → Sequence No help to rearrange the data gram (ordering data gram).
- Sequence Number ⇒ Ordering information for sequence of datalayer


AL
TL
NL
DL
PL
Message
Datagram
Packing
Framing

24/04

PGP (Pretty Good Privacy) Protocol

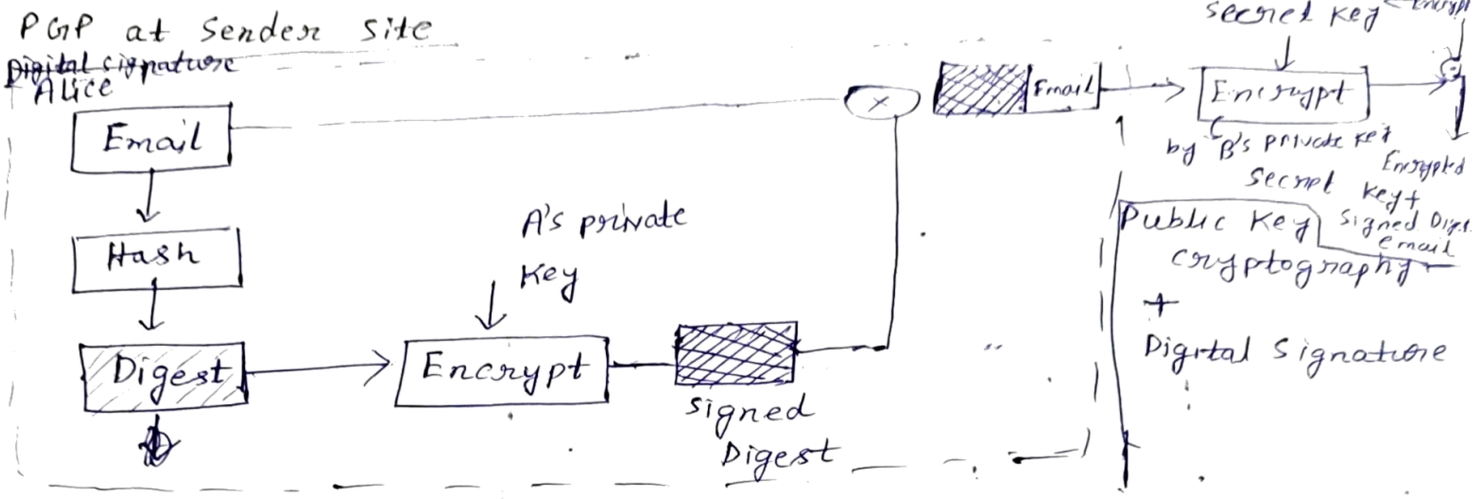
1) Privacy
2) Confidentiality
3) Integrity

TPSEL
TLS
PGP

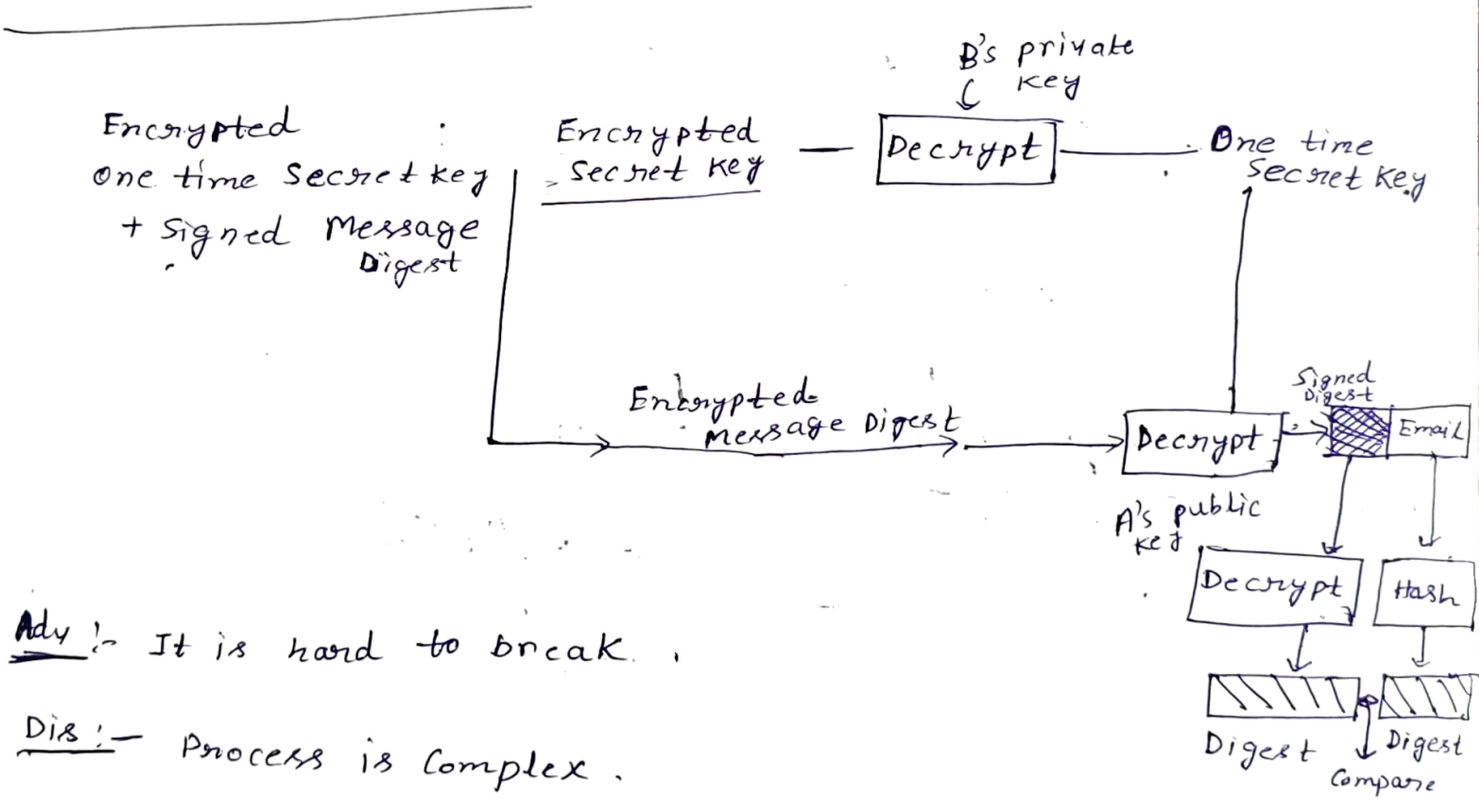
S/MIME
Email

Privacy path

PGP at Sender site



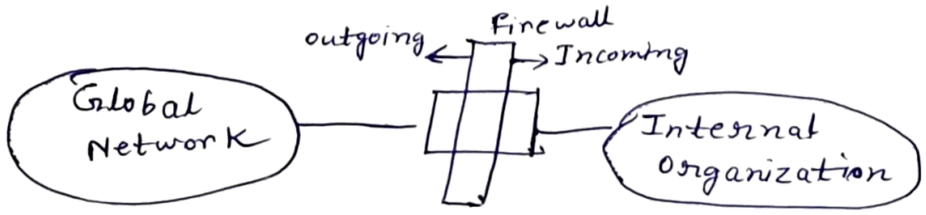
PGP at Receiver site



Adv :- It is hard to break.

Dis :- Process is complex.

Firewalls :- How to protect the system itself.



Firewall is a device (it could be router) installed between the internal network of an organization & the rest of the internal.

Types of Firewall

Two types

- Packet filter firewall
- Proxy firewall

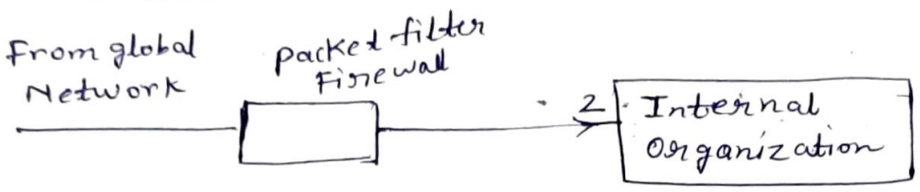
Difference

Packet

Filter the network or transport layer

but Proxy firewall filter the application layer

Firewalls Packet filter



Interface	Source IP	Destination IP	S Port	D Port
1	123.34.5.10	*	*	*
1	*	*	*	23
1	*	*	*	*
2	*	*	80	*

Proxy firewall