Network security

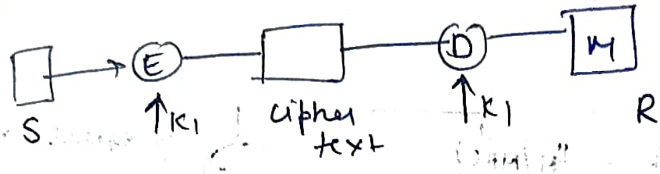
Authentication - An authenticator authenticate the message.

authenticator is a function.

Types - message encryption
MAC (Message authentication code)
Hash function.

1) Message encryption

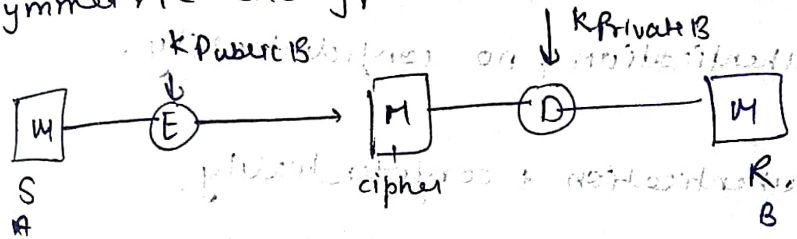
1)



K_1 is shared b/w sender and receiver.

for asymmetric encryption.

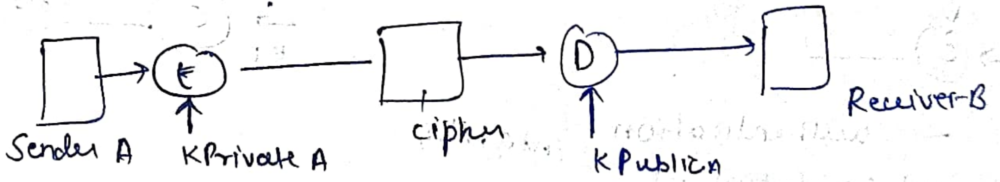
i)



authentication — x

confidentiality — ✓

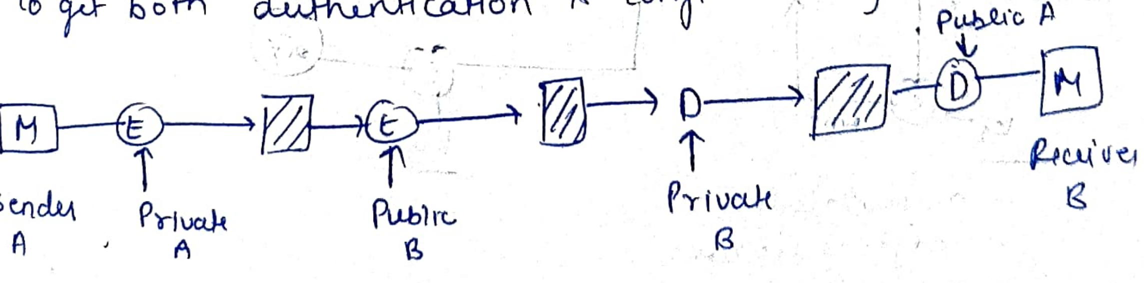
ii)



authentication ✓

confidentiality x

To get both authentication & confidentiality

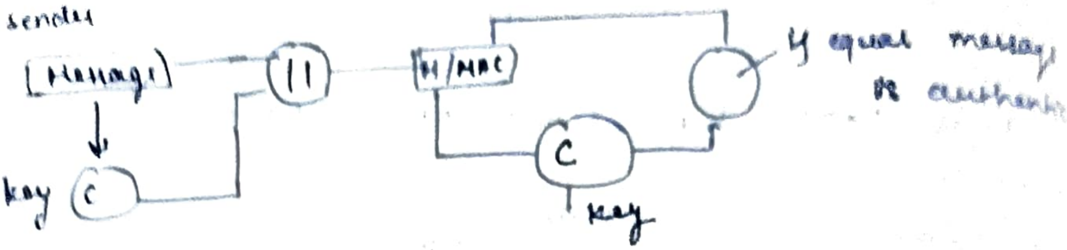


MAC (Message authentication code)

we will have secret key to generate a small fixed size block of data called MAC or cryptographic checksum

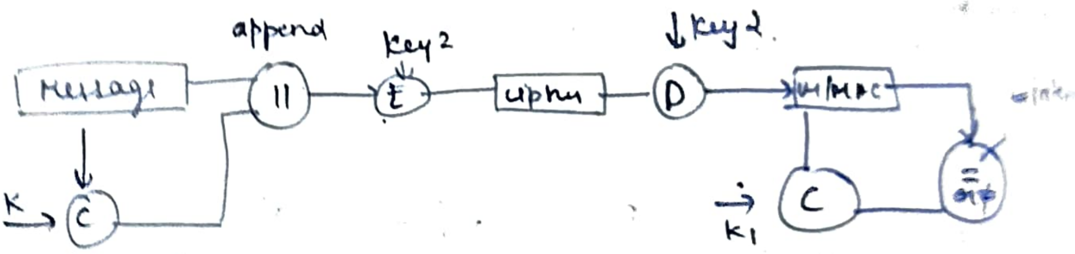
Appended with checksum
communicating parties share secret key

$$\text{MAC} = \underset{\text{function}}{C}(\overset{\text{key}}{K}, \underset{\text{Message}}{M})$$



only authentication, no confidentiality.

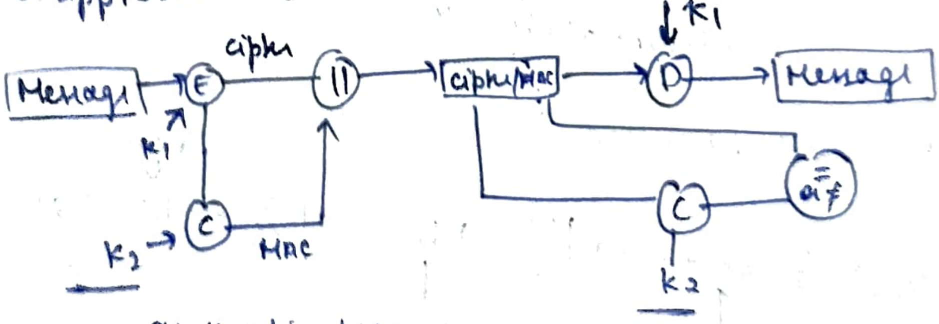
2) MAC - authentication + confidentiality.



→ authentication
→ confidential.

integrity

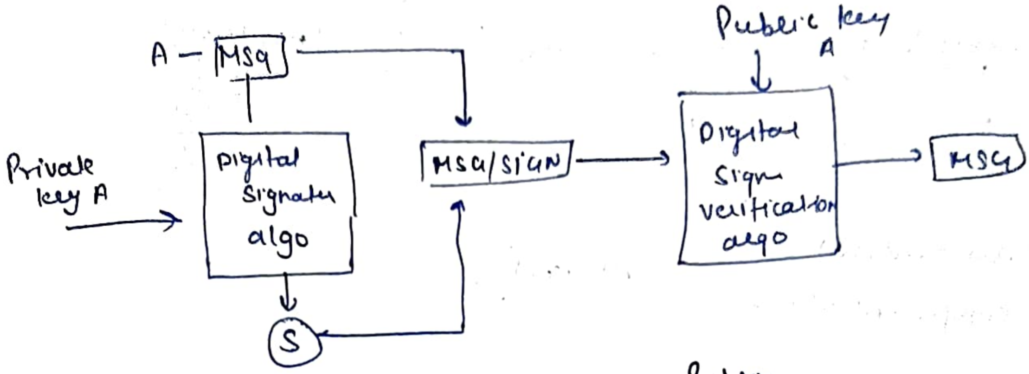
Other approach. (tied to cipher)

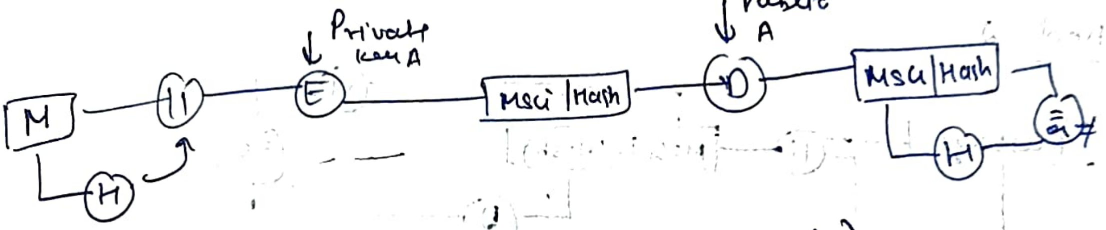


- authentication
- confidentiality
- integrity.

Digital signature - A digital signature is a mathematical technique used to validate authenticity and integrity of a message or digital document.

- Based on asymmetric key
- used for authentication & non repudiation & integrity.
- not for confidentiality





to check for integrity. (using hash)

*. when we sign a document digitally we send signature as separate document. send send 2 document $\overset{(1)}{\text{msg}}$ / $\overset{(2)}{\text{signature}}$

- easy to produce and verify digital signature.

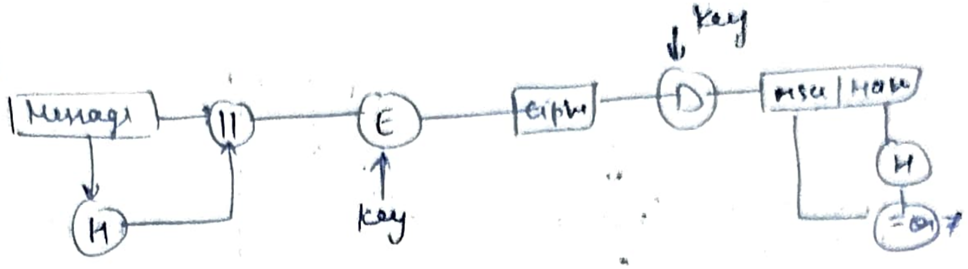
Hash functions -

- similar to mac but it does not use a key
- independent of key.

H(M) = hash code.

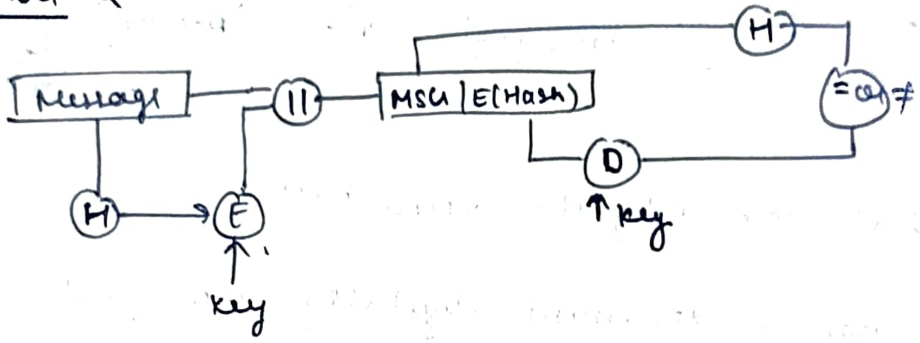
- Produce fixed size code.

i)



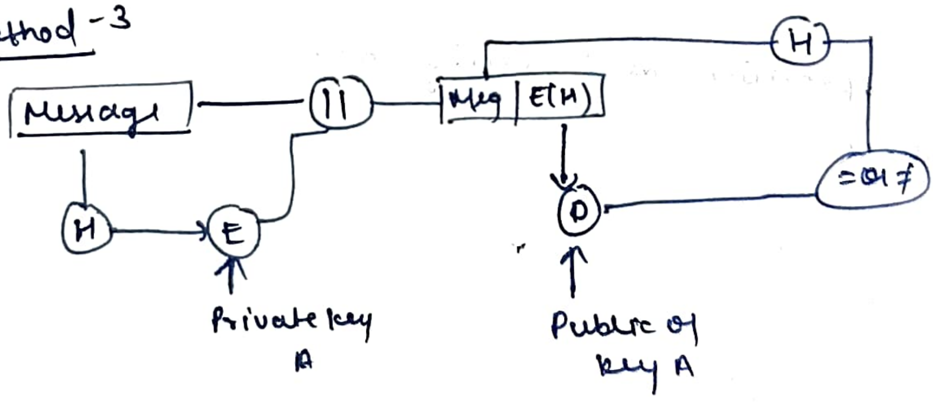
- authentication - integrity.
- confidentiality

Method -2



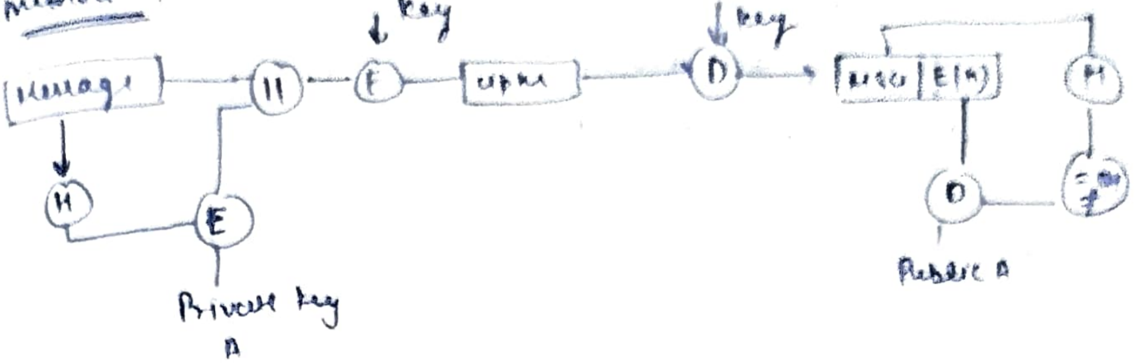
- only authentication
- No confidentiality.

method -3



→only authentication
→no confidentiality.

Method - 4



- authentication + confidentiality.

Message authentication Requirement -

↳ why message authentication is required because of following attacks

Revelation - releasing msg to someone not having key

Analysis of traffic - discovery of pattern of traffic b/w parties. the number and length of msg could be determined.

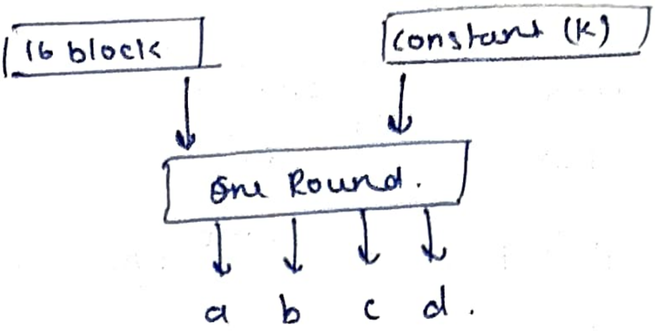
Modification in the content - change content of msg.

Modification in sequence - change of order of msg.

modification in timing - delay of msg b/w parties cause session tracking disruption.

source refusal - source denies to be originator

destination refusal - receiver deny acceptance.



$a = b + ((a + \text{Process } P(b,c,d) + m[i] + T[k]))$

<<shift

secure hash algorithm.

It is a modified version of md5

O/p is message digest of 160 bits in length.

Properties.

- Generating original message from digest
- finding two message generating same digest

} infeasible.

working - i) Padding (64 bit less than exact multiple of 512)

ii) Appending length

iii) dividing the I/p into 512 bit blocks

iv) five chaining variable (A, B, C, D, E)

v) Process Block. - copy of chaining variable

\ 512 - ~~16~~ 16 block

└ four round.
(20 step)

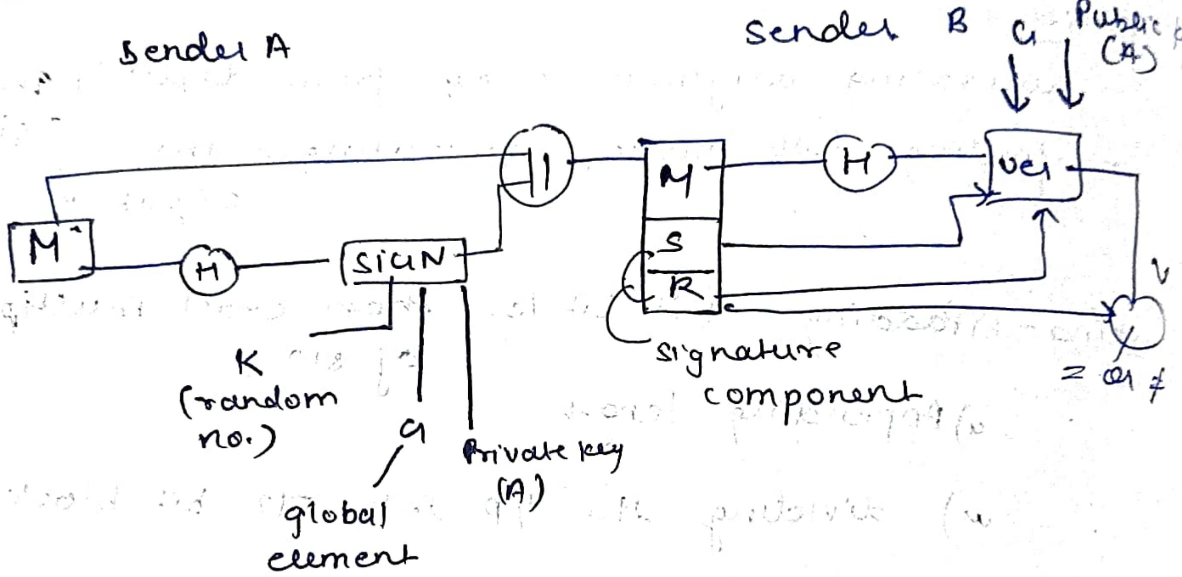
$abcde = (e + \text{Process } P + s^5(a) + w[*] + K[*])$

$, a, s^{30}(b), c, d.$

Comparison b/w md5 & SHA

	MD5	SHA
length in bit	128	160
Attack to find original msg	2^{128} operation	2^{160} operation.
successful attack	Possible.	No such claim
speed	fast	slow more secure

Digital signature standard



global key component

P – Prime no.

$2^{L-1} < P < 2^{L}$

$q \rightarrow$ prime divisor of $(P-1)$

$g \rightarrow h^{(P-1)/q} \bmod P$.

$1 < h < p-1$

user private key

x – Random number

$0 < x < q$

Public key

$y \rightarrow g^{x} \bmod P$

signature

$r \rightarrow (g^{k} \bmod P) \bmod q$

$s \rightarrow [k^{-1} \{H(M) + xr\}] \bmod q$

$0 < K < q$

verification -

$$v = [g^{u_1} y^{u_2} \bmod P] \bmod q.$$

$$u_1 = [H(M')w] \bmod q$$

$$u_2 = (r')w \bmod q$$

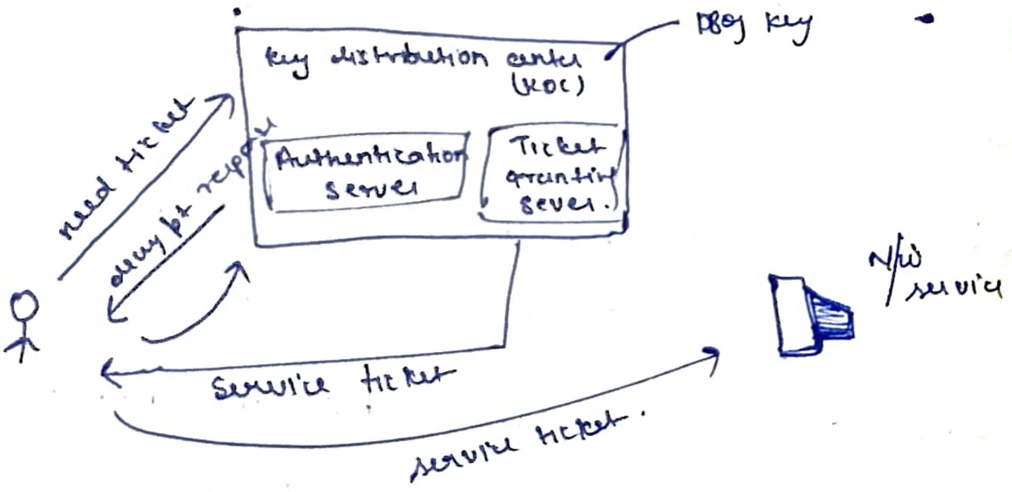
$$w = (s')^{-1} \bmod q.$$

Authentication Protocol

- mutual authentication protocol
- one way authentication
- DSS

Kerberos - It is authentication protocol which works on the basis of ticket to allow nodes communicate over a non-secure N/w to prove their identy to one-another.

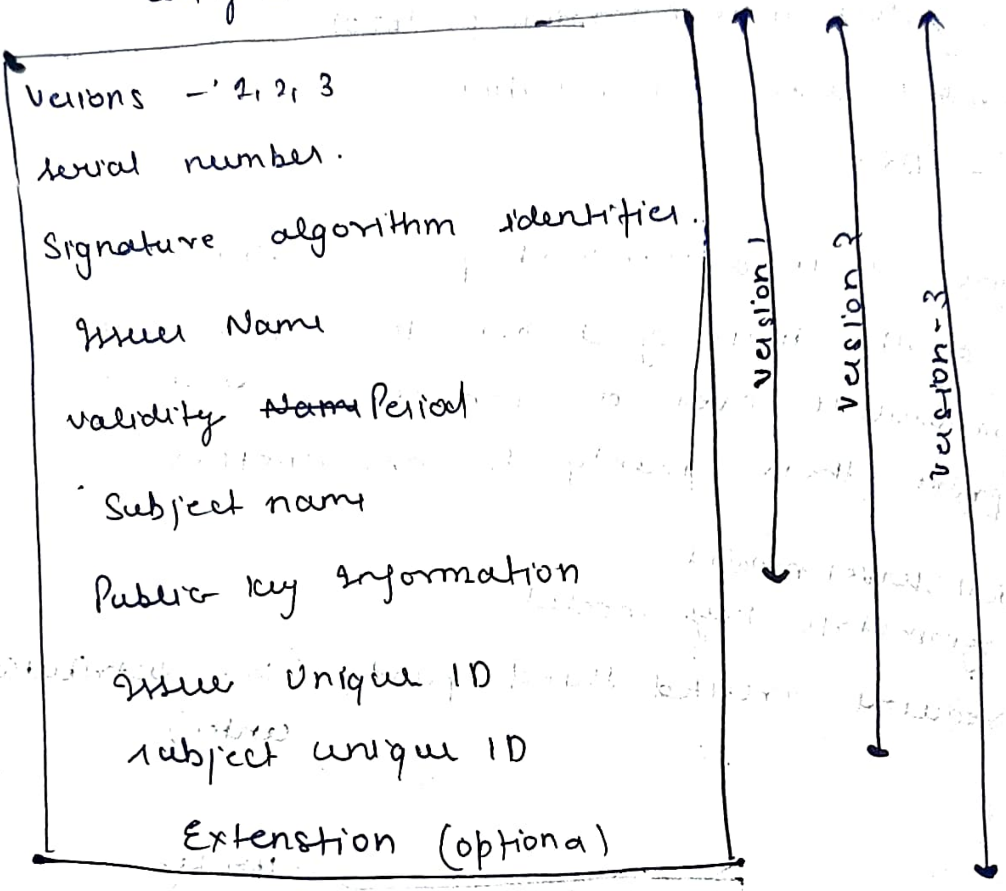
- client server model
- symmetric key model
- requires trusted third party (key distribution center)



X-509 authentication service;

- digital certificate accepted internationally
- does not generate key but provides a way to access public keys.

There are several element in X09 certificate.



Versions -' 1, 2, 3

serial number.

Signature algorithm identifier.

Issuer Name

validity ~~Name~~ Period

Subject name

Public key information

Issue Unique ID

subject unique ID

Extenstion (optional)

one-way authentication

→ { message (A → B) used to establish identity of A and message is from A.

→ message must include timestamp, nonce, B' identity and signed by A

→ may include info of B (session key)

Two way authentication

- 2 message (A→B) (B→A) reply from B.
- reply includes original nonce from A also, timestamp. and nonce from B
- may include additional for A.

Three way authentication

- 3 message (A→B) (B→A) (A→B)
- has reply from A back to B containing signed copy of nonce from B
- means timestamp need not be checked

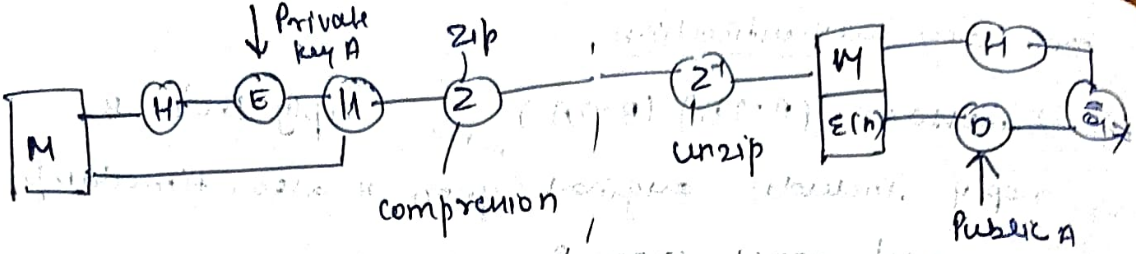
PGP (Pretty good privacy)

- provide email security.
- it is an encryption program that provides crypographic privacy and authentication for data communication.

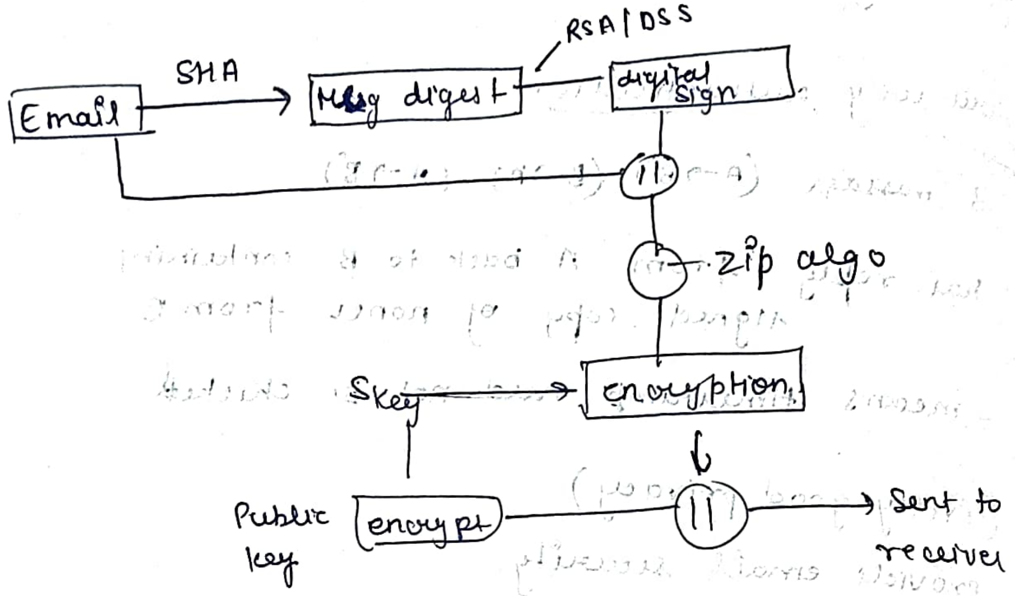
PGP uses

i) data compression
ii) hashing
iii) symmetric key cryptography
iv) asymmetric key cryptography.

each step uses one of several supported algo like RSA, IDEA, SHA.



authentication but not confidentiality.



S/MIME

- Secure / Multipurpose internet mail Extensions.
- provide for commercial mail
- extension of mime protocol
- widely accepted method for sending digitally signed and encrypted message.
- Based on asymmetric key encryption.

Function - - provide authentication
- message integrity
- Non repudiation
- privacy
- data security (encryption)

before S/MIME, SMTP was used which was not secured.

Security services provided by S/MIME

- digital signature (provide authentication & non repudiation)
- msg encryption - confidentiality & data integrity.

MIME - multipurpose internet mail extension.

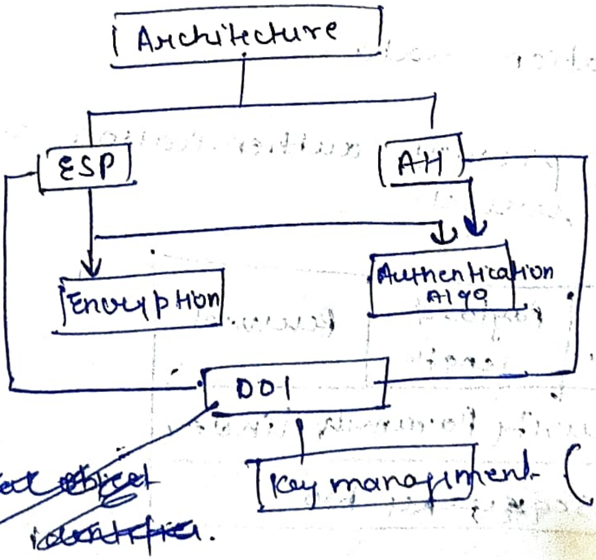
- Email can send only in NVT 7 bit ASCII format
- Nowaday with MIME we are able to send audio, video, images, etc.

IP (sec) Architecture

IPSec (IP Security) has two protocols to secure traffic or data flow.

- ESP (encapsulation security protocol)
- AH (Authentication header)

It provide - confidentiality, Authentication, Integrity.



(how key are exchanged)

~~Digital object identifier.~~

Domain of Interpretation. (identifier suppor AH & ESP protocol).

ESP protocol - It provide confidentiality service. can be implemented in two ways -

- ESP optional Authentication
- ESP authentication.

Packet format -

Security Parameter Index		
Sequence No		
Payload data		
Padding	Padding length	Next header
Authentication data		

SPI - Parameter used to give unique number to client & server.

Sequence No - Sequence number allocated to each packet.

Payload data - actual data

Padding - extra bit added to ensure confidentiality.

Next header - next palyload.

Authentication data -

AH - protocol provide authentication and integrity service.

Next header	Payload length	Reserved
Security Parameter Index		
Sequence No		
Authentication data		

Authentication Algorithm - set of document that describe algorithm used for AH and for authentication of ESP. (SHA, md5)

web security

- web is used by business, government and individual
- but web is vulnerable
- have variety of threat.
  - integrity
  - confidentiality
  - denial of service
  - authentication

  - SQL injection
  - cross site scripting.
- need added ~~secu~~ security mechanism

SSL (Secure socket layer)

- Internet protocol for secure exchange of information b/w browser and server.
- Provide security at transport layer.

goal- confidentiality, integrity, authentication.

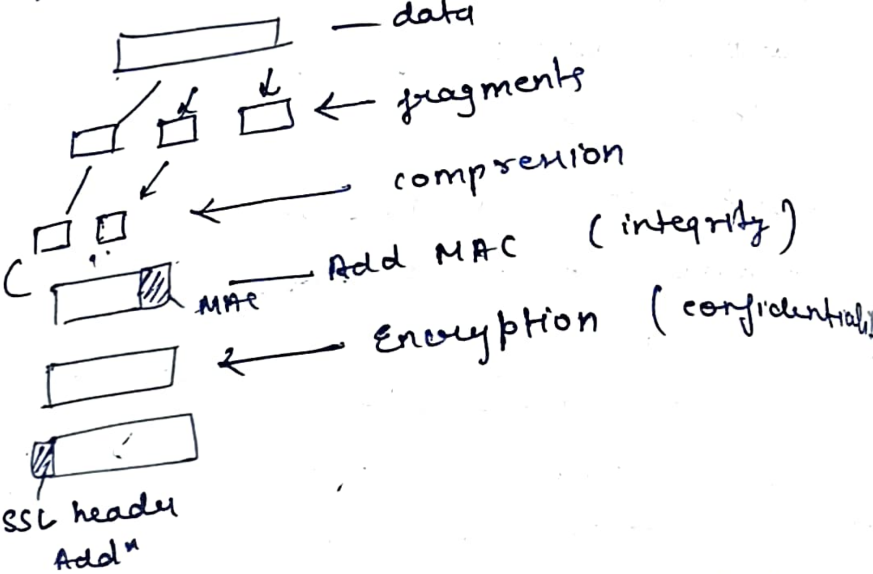
working - contains SSL- Handshake Protocol
SSL change cipher. Spec
SSL alert Protocol
HTTP

SSL architecture

<table>
<tr><td>SSL Hand-shake</td><td>SSL-cipher sec</td><td>SSL alert</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL Record Protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

→ SSL record protocol

- Provides
  confidentiality – Encryption
  message integrity – Hash.



→ change cipher sec Protocol – It consist of a single ~~the~~ message consisting single byte value 1

- cause pending state to become current
- hence updating cipher in use.

→ Alert protocol – convey SSL related alert to peer entity

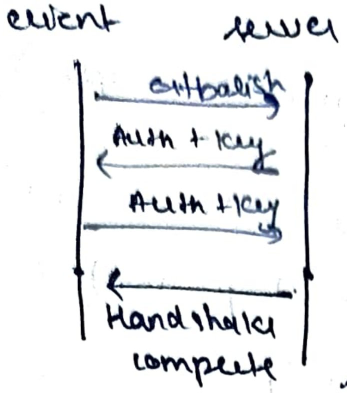
- warning or fatal.

Byte-1 – 1 mean warning
– 0. fatal error.

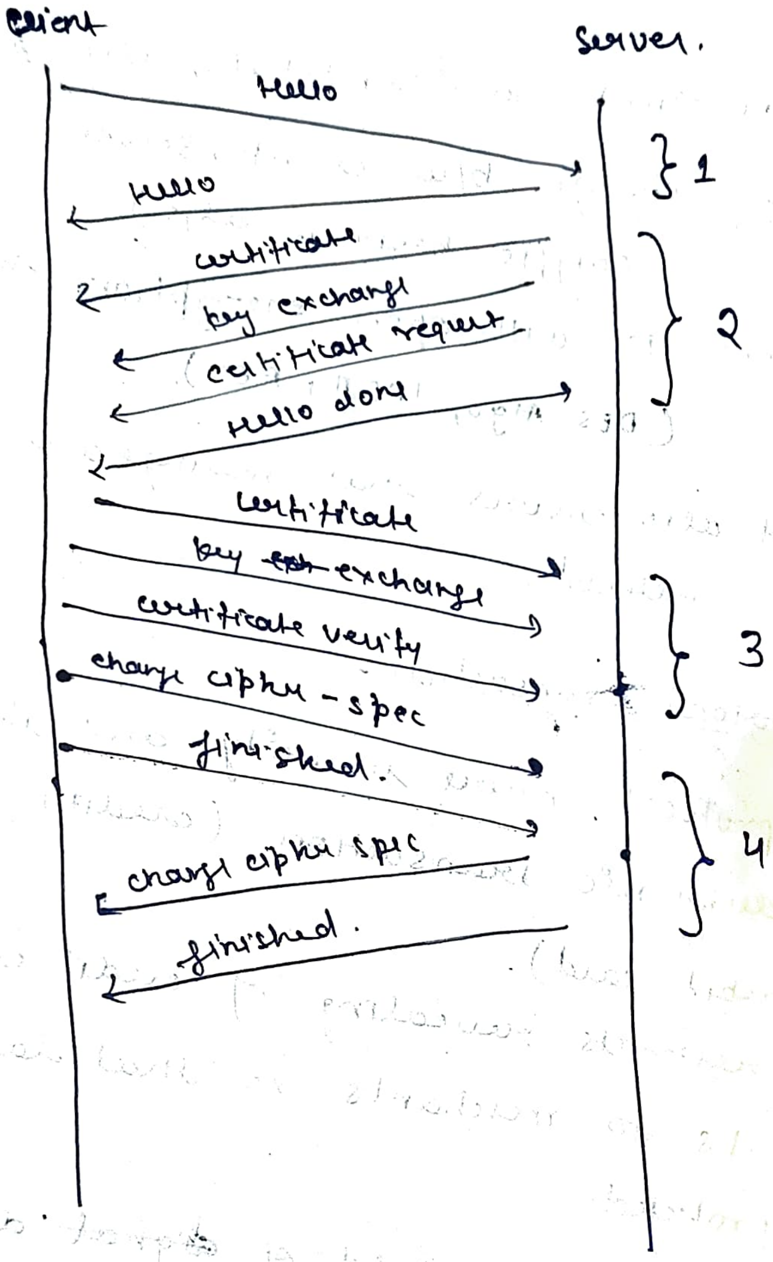
Byte-2: Type of the alert.

→ Handshake Protocol –

- complex part of SSL ...
- Authentication b/w client & server.
- Negotiation of Encryption /MAC algorith
- Exchange of keys.


client
server
establish
Auth + key
Auth + key
Handshake compete

simpler


Client
Server.
Hello
Hello
certificate
key exchange
certificate request
Hello done
certificate
key ~~exh~~ exchange
certificate verify
change cipher-spec
finished.
change cipher spec
finished.
1
2
3
4

Transport layer security

- provides security in transport layer.
- derived from SSL
- provides secured connection b/w client and server. (no third party).
- It is used by HTTP, SMTP.

working

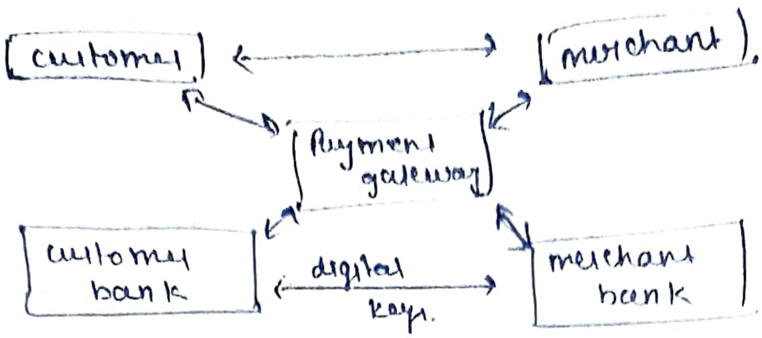
- uses client server handshake mechanism
- key exchange b/w client, server. (diffie helman algo)
- Now HS will open encryption channel (DES Algo, IDEA, AES)
- It also ensures that message are not altered.

Secure Electronic transaction -

→ This protocol ensure security and integrity of electronic transaction (credit, debit card).

→ Set restricts revealing of credit card details to merchants so that data in protected

→ implemented with need of ~~dignat~~ digital signature.



<u>system security</u> - security of computer ~~[illegible]~~ system is crucial task. It is process of ensuring the confidentiality and itegrity of the OS. Security is imp to key all threat alway from computer software system.

Intruder are attackers who attempt to breach the security of network.

└ Types - masquerader - outsider aims to attack unethically by stealing data / info.

- misfeasor - authorised to use system but misuse granted access.

- clandestine - that have supervision control of system and misuse authoritative power of them.

Threat - program that has potential to cause serious damage. to system

Attack - an attempt to break security.

<u>Threats</u> - virus, trojan horse, worm, trap door.

Trusted computer System

- A system that has the necessary security function and assurance that security policy will be enforced, and that can process a range of information sensitivities
- enables subjects (people or program) having varying right of access to objects.
- multilevel security (- Top level
  - Secret level
  - confidential level
  - unclassified level)

importance - Identity verify
safety maintained
limited access.

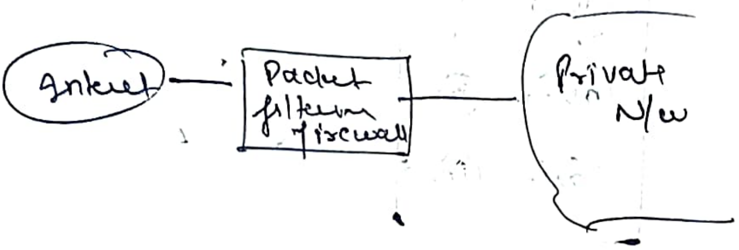
firewalls - A network device
- Hardware or can be software
- All data pass through firewall.
- after examining the data, firewall either block or pass the data.
- It is barrier b/w secured N/w & outside network,

Type of firewall

1) Packet filtering firewall
2) Application ~~lev~~ level gateway
3) circuit level gateways.

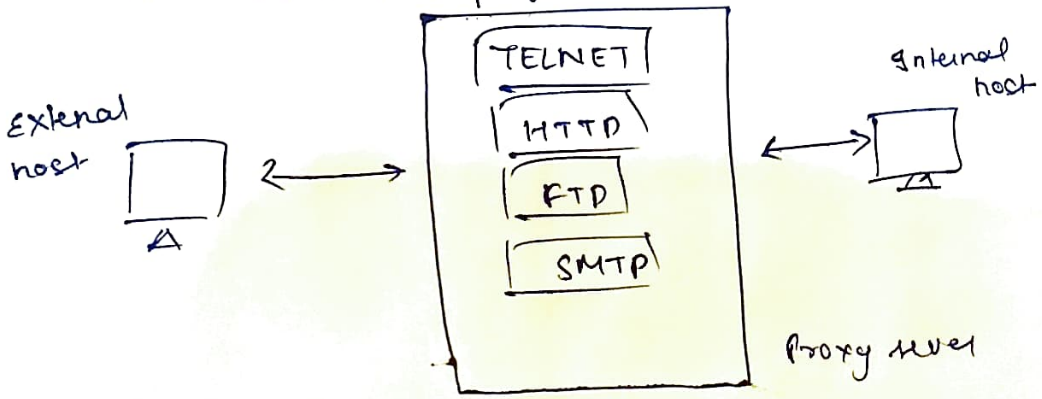
Packet filtering firewall

- Applies set of rules at each incoming IP packet and then forward or discard packet
- Rules are based on source IP, destination IP protocol & port
- If rule matches, corresponding action will be taken
- otherwise discard
- It analyse traffic at transport layer.
- maintains filtering table.



Application level gateways

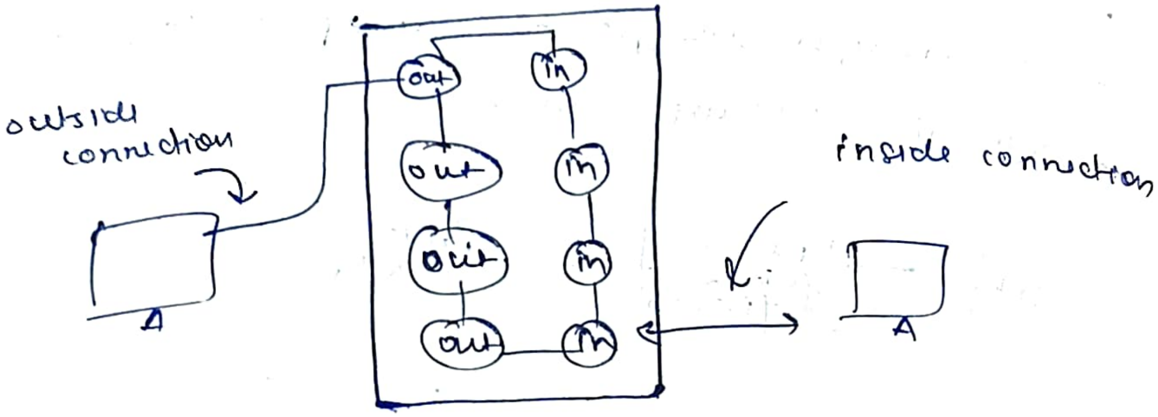
- also called proxy server.
- contact user using TCP/IP application like (TELNET, FTP, HTTP, SMTP etc)
- more secure than packet filtering & layer.
- processing overhead.
- check data and payload.



circuit level gateway

- uses two TCP connections
  - i) b/w internal host and gateway
  - ii) b/w external host and gateway.

Security check done before setting up a connection. once connection is established all the data will be passed.



circuit level gateway

Advantages

faster than application level gateway.

md5 message digest algorithm

↳ developed by Ron Rivest

↳ fast and produces 128-bit message digest.

working - i) Padding (Padding is done such that total length is 64 bit less than 512 multiples).

1000 bit

512×2 =1024 add 472.

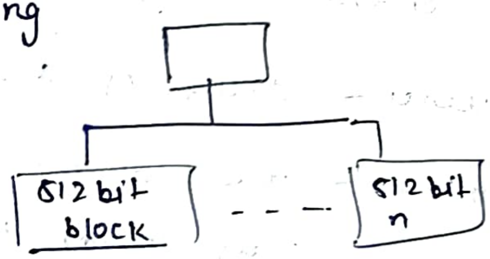
512×3= 1536
−1000
− 64
472

ii) Append original length before padding (% 64)

most of cases 64 bits is obtained,
append 64.

so, it becomes multiple of 512.

3) dividing



1024
/ \
512 512

4) initialising (4 chaining variable)

each 32 bit

a,b,c,d predefined value.

5) Processing (512 bit block)

copy chaining variable.

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

divide 512 bit 16 block of 32 bit.