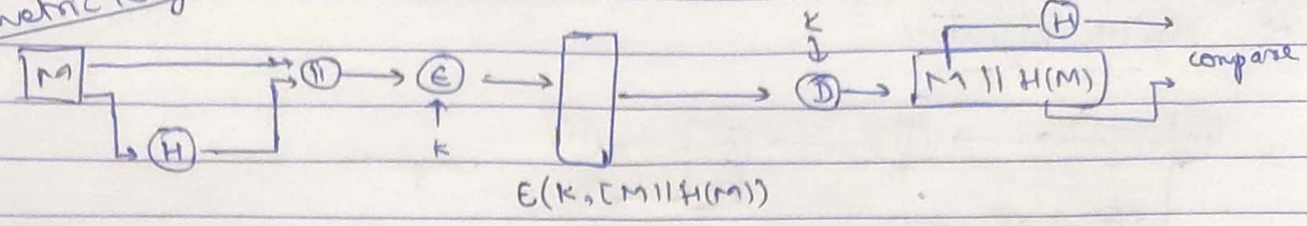
msg + hash code + encry → confidentiality

Hash functions: (give confidentiality)

Symmetric key

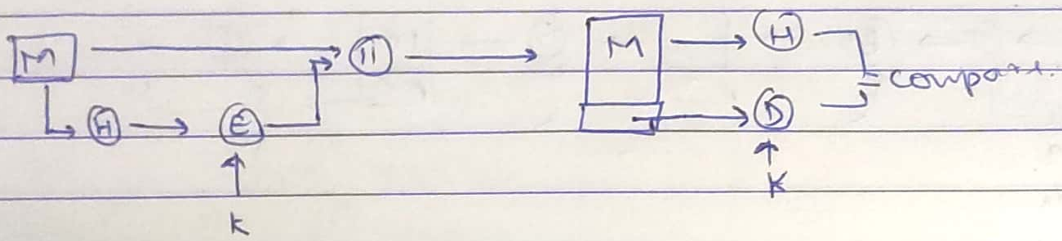
①



→ confidentialy is provided by cz of symetric key as this key is present only to authorised person.

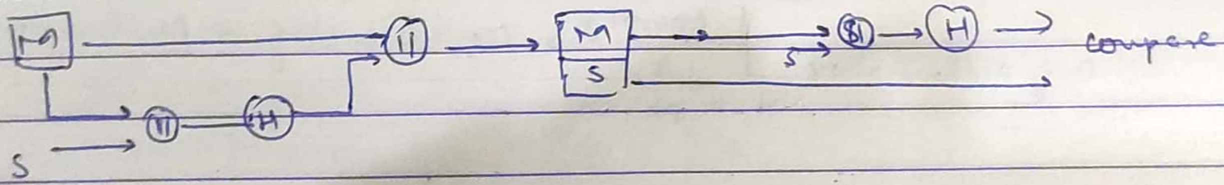
→ Hash code is used for authentication.

②



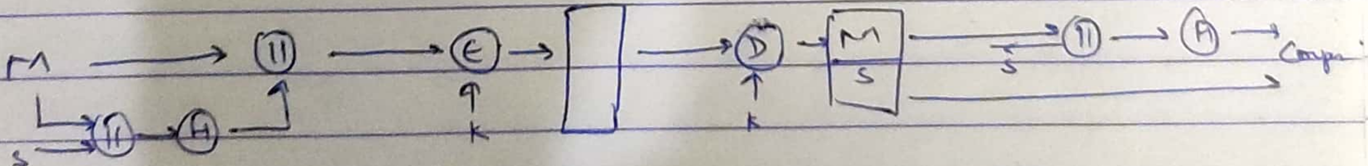
No confidentiality ⤴

③



No confidentility ⤴

④

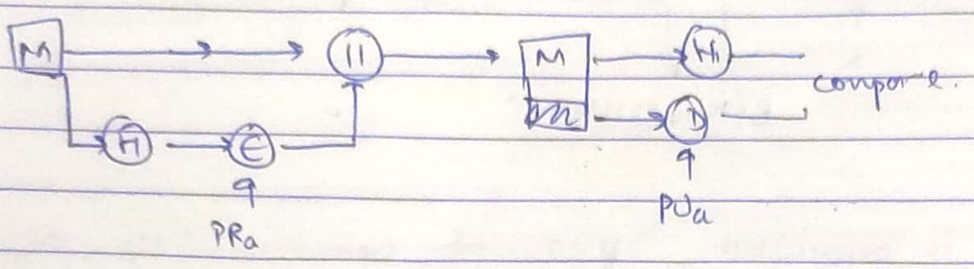


confidentiality + authentication ✓ (msg + hash) → (Encrypt)

↑ K ↑ K

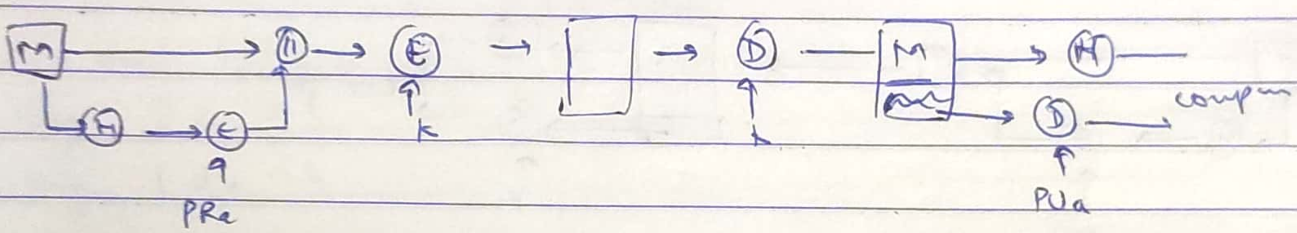
(Assymetric key)

→ Digital signature.



Authentication ✓

For cofidenciality



So conclusion → Hash prodives integrity by default

→ if ~~the~~ Msg + Hash

Encrypty, confidiently + Authenticati

Only Authentication Not encrypt

Formulae:

RSA →

- $n = p * q$
- $\phi(n) = (p-1)(q-1)$
- choose e $1 < e < \phi(n)$ $\gcd(e, \phi(n)) = 1$
- calculate d

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

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

- Public key $\{e, n\}$
- Private key $\{d, n\}$

- En : $C = M^e \bmod n$
- De : $M = C^d \bmod n.$

↔ Deffie Hellman

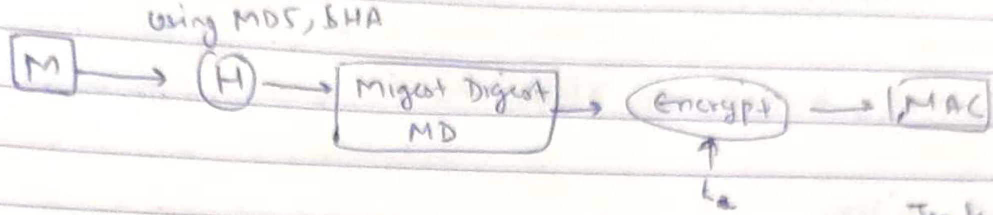
- Let prime q
- primitive root $\alpha.$ $\alpha < q$
- Assume Private key X_A, Y_A

- Public key = $Y_A = \alpha^{X_A} \bmod q$

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

- key tobe used $= Y_B^{X_A} \bmod q = Y_A^{X_B} \bmod q$

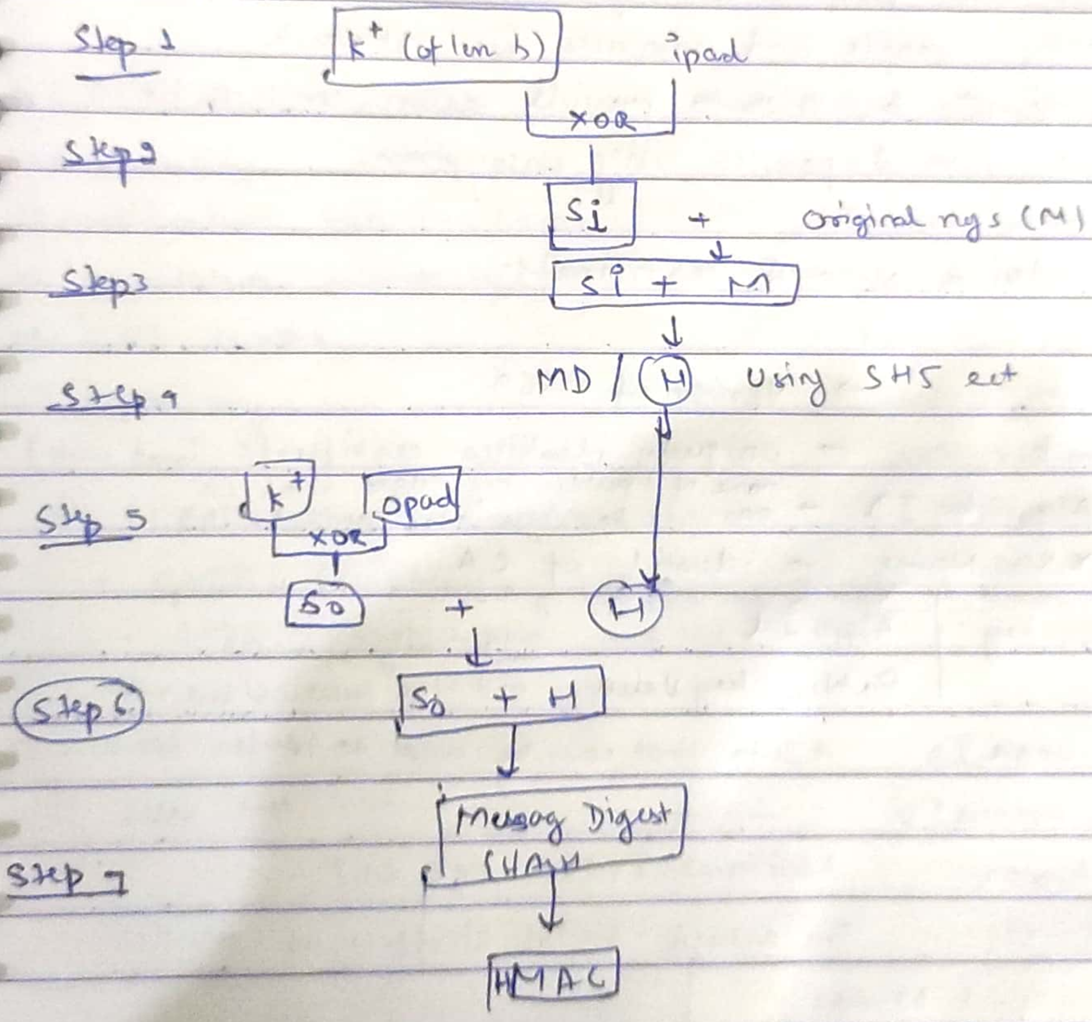
HMAC Hash msg Auth code



Integrity + Authentics

ipad → (36 in hexa) 00110110

opad → 5C in hexa 01011100



$$HMAC(k, m) = H[(k^{+} \oplus opad) \| H[(k^{+} \oplus ipad) \| m]]$$

Other topic → DAA (Data Authentication Algo)
→ CMAC [Cipher Based Msg Authentication Code)

These both are based on Block cipher

see ppt and video:

X.509 Certificate:

Purpose → The main purpose of digital certificattes (SSL/TLS) is to identify people and resources over network such as Internet & also to provide secure, confidential communication b/w 2 parties using encryption.

See ppt for detailed view of certificate.

Version → Version of X.509
Serial Number → uniquely identifies certificate (not user)
Signature Algorithm ID → name of public key algo that CA has used to sign certificate (RSA)
Issuer (CA) X.500 Name → identity of CA
Validity Period Subject X500Name → ~~owners identity within X.500 directory~~
Subject Public key Info | Algo Id
| Public key Value ~~Public key of owner~~ and algo associated to it
Issuer unique ID → Info that can be used to identify issuer
Subject unique ID ———— ident user
extension Additional Info CRL, CDP
CA dig. sig. The actual digital signature of CA

Version Serial Numbe	
Algo used to sign certificate.	websites have certificates
Identity of CA Validy Period	issued by servers.
Identity of owner	
Public key and algo used.	
Verify id of CA	
Verify Id of owner other (Extension)	
signature	

→ Public key Infrastructure:

→ set of { hardware, software, policies, procedure, people } needed to {create, mange, store, distribute, revoke digital certificates}

→ Public key Infrastructure X.509 is calles (PRIX)

→ PRIX Elements:

CRL (Certification Revocation List).

Full Ratta, read PPT.

* PRIX Elements:

→ End entity

→ Certification Authority (CA)

→ Registation Authority (RA)

→ CRL issuer

→ Repository.

* PRIX Managment. Functions

- Registration
- Initialization
- Certification
- Key Pair Recovery
- Revocation Request
- Cross Validation.

* PKI Managa Protocols.

- CMP (certificate managment Protocol) → request, revoke, suspend, resume
- CMS (Cryptographic message syntax) → encrypt decrypt sign verify compress decompr

Kerberos: Kerboros is a network authentication protocol that works on basis of tickets to allow nodes ~~to~~ communicating over non-secure network to prove their identity to one another in a secure manner.

3 heads! 3 step process:

→ Authentication as per → (1) User
→ Authorization video (2) KDC
→ Accounting (3) Services.

Requirement of kerberos

- Secure
- Reliable : one system able to back up another.
- Transparent:
- Scalable : modular distribute architecture

→ KDC → The service that offers Kerbos ticket

→ Ticket Granting server (TGS): A server that issues tickets for desired services which in turn are given to user to access the services. Runs on same host as KDC.

* Kerberos is capable of both symmetric and asymmetric techinques.

Kerberos is more secure than other authentication methods because it doesn't send plain text password over internet and instead uses encrypted tickets

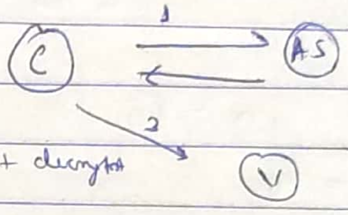
Kerberos 4.

2 ways

(1) Using Authentication server only

(2) Using AS + TGT (Ticket granting server).

(1) Using AS.



(1) R → AS

(2) AS → C : Ticket

Encrypted, Client can't decrypt

(3) C → V $ID_C \,||\, Ticket$

Server will match ID_C which means Identity of client is verified.

(1) C → AS : $ID_C \,||\, P_C \,|\, ID_V$

(2) AS → C : Ticket $E(K_V, [ID_C \,||\, AD_C \,||\, ID_V]$

(3) C → V : $ID_C \,||\, Ticket$.

V (Server) will match them and then start communication on AD_C.

(✱) Problem : (1) User would need ticket for every new service.

(2) password is transmitted without encryption.

Elgamal Algo:

global elements of Elgamal digital signature is based on prime number q and α, which is a primitive root of q.

→ Generate private key & public key.

→ X_A $\qquad 1 < X_A < q-1$

eg $\quad q = 19$, $\alpha = 10$ $\qquad$ q, α → global elemetns

let $X_A = 16$.

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

$Y_A = 4$. $\qquad$ A public key = $\{q, \alpha, Y_A)$

so ~~Y_A is public key and~~ $\qquad$ X_A → private key

Y_A → public key.

let Sender wants to sign a hash value $m = 14$

→ Create digital signature

- Choose k $\qquad 1 \le k \le q-1 \qquad \gcd(k, q-1) = 1$

Let $k = 5 \qquad \gcd(5, 18) = 1$

$S_1 = \alpha^k \bmod q \quad = 3.$

$S_2 = k^{-1} (m - X_A S_1) \bmod (q-1)$

$= 5^{-1} (14 - (16)(3))\% 18 = \quad -374 \bmod 18 = 4$

Signature consists of $(S_1, S_2) = (3, 4)$.

$5^{1} \bmod 18$ $5^{17} \bmod 19$

$5^{18} \bmod 19 = a \times 5^{i}$

→ Signature verification :-

$5^{17} \bmod$

$V_1 = \alpha^{m} \bmod q$

$= 10^{14} \bmod 19 = 16$

$V_2 = (Y_A)^{S1} (S_1)^{S2} \bmod q$

$= 4^{3} \; 3^{4} \; \% \; 19 = 16.$

$V_1 = V_2 = 16.$ both the values are same.

In a nutshell :

Assume q and α.

- Select X_A → private key
- Find $Y_A = \alpha^{X_A} \bmod q$
  Public k $\{q, \alpha, Y_A\}$
- Given hash value m
- Chose K $(1 \leq K \leq q)$. $\gcd(K, q-1) = 1$
- Find $S_1 = \alpha^{K} \bmod q$
- Find $S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$

Signature conists of (S_1, S_2)

$V_1 = \alpha^{m} \bmod q$

$V_2 = (Y_A)^{S1} (S_1)^{S2} \bmod q$

$V_1 = V_2$.

p and e_1

d

public key. $e_2 = e_1^{d} \% p$

(e_1, e_2, p).

m

r

$S_1 = e_1^{r} \bmod p$

$S_2 = r^{-1}(m - d S_1) \% p-1$

$V = e_1^{m} \% p$

$V_2 = e_2^{S_1} S_1^{S_2} \bmod p$

$5^{-1} \bmod 18$

$a * b = 1$

$(a * b)$

~~$a x \% m = 1$~~

5×5

5^{-1}

$5^{-1} \% 18$

$a x \% \bmod m = 1$

Security Assocation:

- → One way relationship B/w sender and reciever.
- → 3 parameter.
  - → security Protocol Identifier (which Protocol AH / ESP?)
  - → IP Destination Address
  - → Security Parameter Index (unique identifies a particular security Associat)
  - → Sequence number counter (0 to $2^{32}-1$) (increment after every Packet is sent)
- → has other Param:
  - → EH, AH info, Key life time
  - → Algo used.
  - → IPsec Protocol mode.

→

Bas inka block diagram nayaa bhayaa ae

JESUS LOVE ME

→

AL
↓
SSL
↓
TL

Secure socket layer (SSL)

- → Lies b/w Application and Transport layer.
- → Ensures conf + authn. + integrity

overview

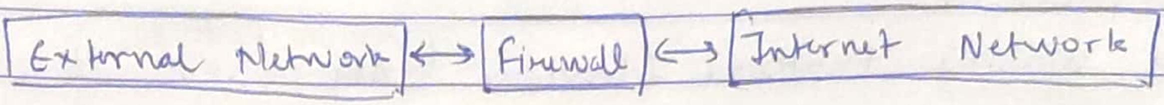
- → 4 Protocols:
  - → Handshake Protocol (Imp) (connection + authen)
  - → SSL Record Protocol (Imp) (conf (Encry) + integrity (MAC))
  - → Alert Protocol (Alert, error msgs)
  - → Change cipher spec Protocol. (1 msg of 1 byte of value 1 Pending state → running state)

bit flip.

Handshake	spec	Alert	HTTP
SSL Record Protoc.			
TCP			
IP			

SSL Protocol Stack

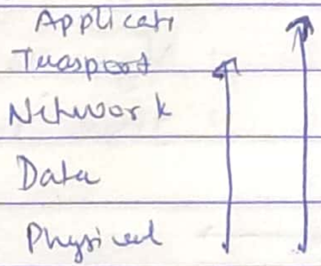
FIREWALL:



→ prevent unauthorise access

→ Monitors and controls incoming and outgoing traffic based on predifined ruls

→ can be software, Network or mixture



Types of firewall.

(1) Packet filtering (layer 4)

→ check IP header, TCP header.

→ Works on Network and Transport layer

→ Can block IP address, full Network

→ ~~tha~~ Can block a service (http, ftp)

→ Source IP, Source Port, Dest IP, Dest Port

~~(2) Application filtering~~

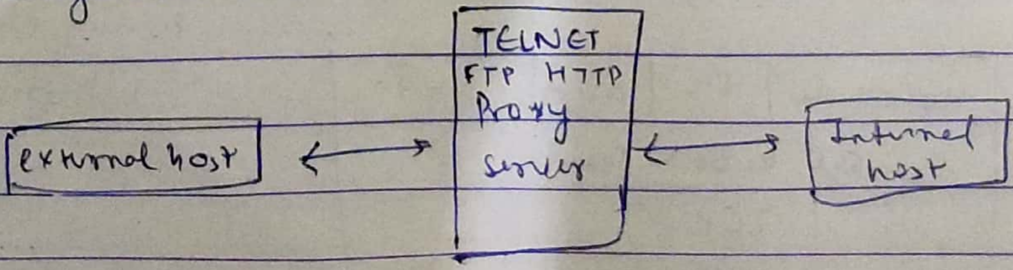
(2) Application-level Gateway (layer 5) (proxy server)

→ data is also verified., check data/Payload. data may contain malacious data.

→ More secure

→ Eg checking email/password on login.

→ processing overhead (Disadvantage)



we think that hum directly external host se contenct me h.
external host thinks ney proxy se a rhi, but bhej hum rahe h

(3) Circuit level Gateway

→ uses 2 TCP connection
  → b/w Internal host ↔ Gateway
  → b/w external host ↔ gateway

→ Security check is done before establish connection

* Intrusion Detection system (IDS)

Intruder (someone with unauthorizd accs) → Outside Intruder (Masquerad
→ Inside Intruder (Misfeasor) (hard to identify)

↓

Intrusion (act of intruders)

↓

Intrusion Detection System (IDS)

IDS methods:

(1) Signature Based IDS:
→ pattern of sig among packets.
→ Database of attack pattern.
→ If signature maches, their is attack.
→ Can't identify new attacks.

(2) Anomaly Based IDS!
-deviation
→ behaviour of people from their 'normal' ~~job~~ behaviour

IDS Types!

(1) Network Based IDS

- → Analysis: Matches traffic to the library of know attack.
- → monitors, capture & Analze network traffic
- → Detect malacious data present into packets.
- → Difficult to do on busy netword.

(2) Host Based IDS

- → installed on device or network
- → monitors packets from device only (to and fro packets)
- → Alert suspious activity (check with ideal system)
- → file deleted or modified.

What is NAT?

Network Address Translation allows a private network to use a set of private address and a set of global Internet address for external communicatio
It uses translation table to route msgs b/w two networks and provides substantial security.

A computer virus is a kind of malacious comp prgm which when executed, replicates itself and modify or insert its own code.