Information Security

Cryptography
- Data Confidentiality
- Data Authentication
- Data Integrity
- ~~Del~~ Entity Authentication
- Trust
- Data privacy
- Anonymity

← Security properties.

Data - that is being stored on Machine + Data in Transit.

Data → static Data (Data privacy)
→ Data in Transit.

- small and critical part in security of Data.

Internet - Many sites are confidential.

private data ≠ Confidential data

- Data is not known to you (No one can access data)
- If you ~~have~~ are given with data you cannot make anything of it. (Even access, cannot understand it)

- Every Data in Transit is prone to capture. (Data Confidentiality)
- Data privacy related to static data (stored in machines/ Hard Disks)
- Confidentiality ≠ Transit data (while communication happening)

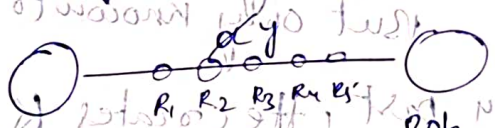
Data Confidentiality:

- Data in Transit.

How to accomplish data Confidentiality?

→ Encryption algorithms.

Key - To distinguish two computers on internet.



$f(x) = y$

- we cannot prevent data to capture.
- f and $f^{-1}()$ are same information theoritically.

$f()$ is known to everybody.

x is known to Alice & Bob (ultimately)

f^{-1} is known to Bob & Alice.

Key - a single person who knows it, others don't know.

$f(K, x) \rightarrow y$ $\quad f^{-1}(K, y) \rightarrow x$.

Development of an Encryption algorithm:

Alice
(1) Has plaintext x
(2) Has Key K
(3) Has encryption function (f_K)

Compute: $y = f(K, x)$ → y → Bob

Oscar
1. Has f
2. Has not Key
3. Has not f^{-1}

okay to relax this condition as Bob never known to Oscar ⇒ has f^{-1}

Bob
1. Has K
2. has f^{-1}
3. Get y.
4. Compute $x = f^{-1}(K, y)$

y — cipher

Both Key and f^{-1} cannot be made available to Oscar!

How K known to Both Alice and Bob?

$f(K, x)$ — information, y - Not information

without knowing Key to Alice how Alice can Encrypt?

A) $f(x)$ ~~only known to Alice~~ known to everyone

$f^{-1}(y)$ — only know to Bob.

$f(x) = y$ → y is given → $f^{-1}(y) \to x$

Computing $f^{-1}(y)$ is difficult but only known to Bob.

Doubt
If oscar has f, how he can't have f^{-1}?

difficult to find K

$y = mx + K$

$x = \frac{y - K}{m}$

$f^{-1}(x) = \frac{x - K}{m}$ → Dependent on K!

1st model - Alice is main part, He creates K and gives it to Bob

2nd ~~Bob~~ model - Bob is main part, Bob creates f and f^{-1}, Alice just gives input to f and Bob decrypt it

If oscar has not know f^{-1} even after knowing f, means oscar cannot calculate f^{-1} from f, it is just known to Alice who calculated it.

Algorithm = Black box where it will be used.

Alice

Bob

Oscar

How Alice can distinguish Oscar and Bob?

option ①

- Key Exchange (Secret information)

option ②

$P = f^{-1}$ and is known only to Bob
$E =$ and f is known to everybody.

Information - No one should know this, If so, Not a information

f - Not a information as it known to everyone.

Ex: $E(K, x)$

$y \leftarrow K \oplus x$

$D(K, y)$

$x \leftarrow K \oplus y$

Encryption has to be associated with Decryption.

→ Assume K has been already shared b/w two parties.

→ Deterministic Algorithm.

$D(K, E_0(K, x)) \rightarrow x$.

Guess: If 256 bits, $\frac{1}{2^{256}}$

- If more messages are sent from Alice to Bob, If any Message is known to Oscar then he can find remaining messages decrypted. $(len(K) = len(message))$

Ex: $E(K, x)$

$K_0 \leftarrow K$

for $(i = 1, i{+}{+}, i \leq l)$

$x \rightarrow x_L \| x_R$ ← broken to two parts

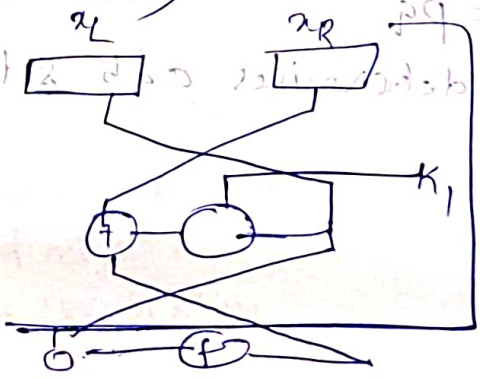
$K_i = K_{i-1}$

$x_L = x_R \oplus (x_L^3 + K_i^3 + K_{i-1}^3)$

$x_R = x_L$

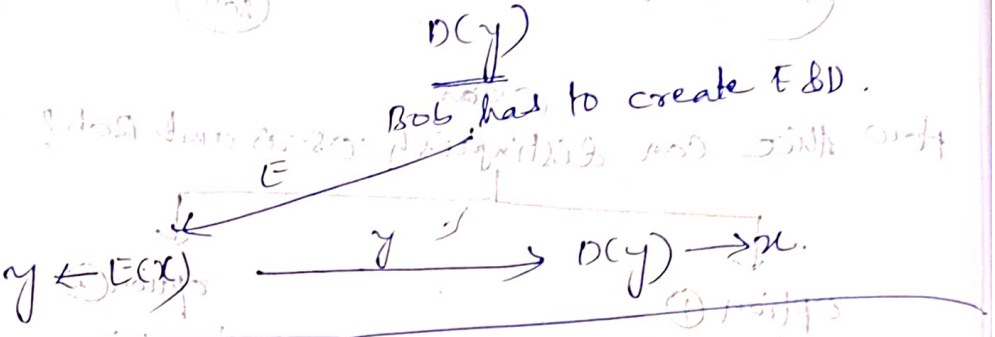
$y = x_L \| x_R$

ciphertext

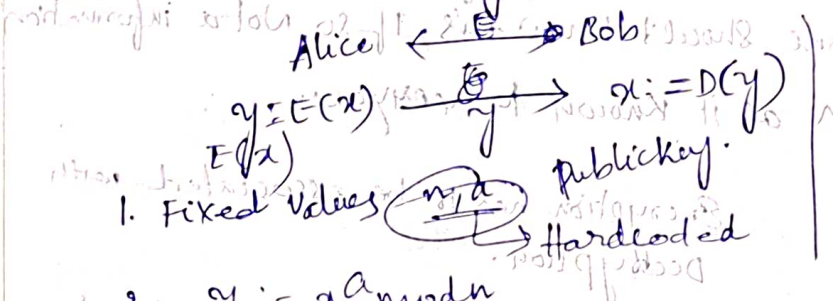


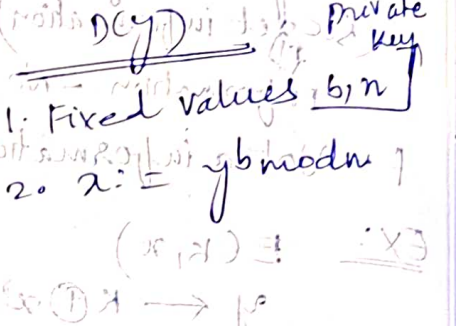
How Bob decrypt y?

- ~~Exact~~ without key



Option 2 (Confidentiality)





- Bob sends E with n, a embedded in it, As (n, a) known to everyone it cannot be a key ~~as it is~~ (public key).

$$x = y^b \bmod n$$

$$x = x^{ab} \bmod n$$

If $ab = 1$,

If $ab = 1 \bmod (p-1)(q-1)$

when $n = pq$

p, q are prime numbers

Bob creates p, q, n, a, b and sends only n, a to Alice.

~~$\phi = (p-1)(q-1)$~~

$(p-1)(q-1)K + 1 = b$

$(pq - p - q + 1)K + 1 = b$

$(n - p - q + 1)K + 1 = b$

Bob in his own computer does the following

- choose p & q (primes)

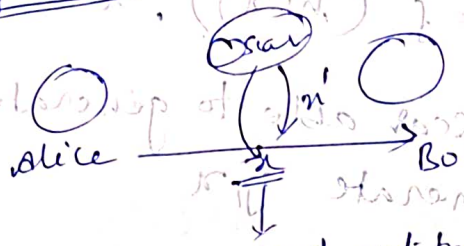
$n = pq$

- Bob determines a & b s.t $ab = 1 \bmod (p-1)(q-1)$

RSA Algorithm

Property 2: Data Integrity

Application:



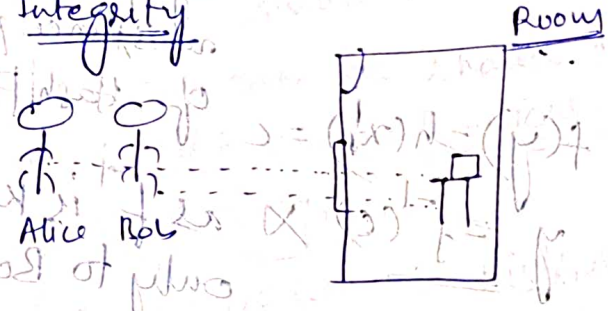
Need not to be encrypted.

How can Bob know if x is tampered in b/w?

Assumption

① Alice and Bob are Honest to each other.

Data Integrity



How Alice ensure that Bob red same file?

- Alice computes $H := h(F)$.

Alice gives H to Bob.

Alice keeps F on table of closed room.

Bob goes and check h(file on the table) and Hash he received from Alice.

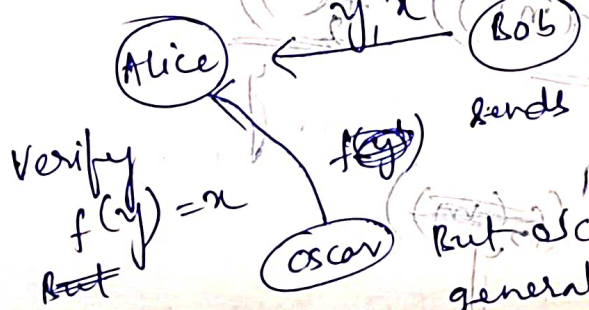
- Integrity can be achieved by Hash function.

Authentication:

we got $E(\cdot,\cdot)$ $D(\cdot,\cdot)$
f, f^{-1}
$h(\,)$

} Design an authentication algorithm using these functions.

Model 1



Bob sends $y' = f^{-1}(x)$ and x

But oscar can take random y' and generate $f(y') = x$ and send it to Alice. Alice cannot differentiate Bob and oscar.

So, not a valid model for authentication.

Model-2

Alice ← y, x ← Bob

$y = f^{-1}(h(x)), x$

problem with the model-1 is Oscar able to generate, y, x s.t $f(y) = x$. Now to generate y, x

let's say $y' = y' \Rightarrow f(y') = h(x)$

$c = h(x)$ ✗ can not find x, by preimage resistance property of hash function.

$x = x' \Rightarrow f(y) = h(x') = c$

$\Rightarrow y = f^{-1}(c)$ ✗ as f^{-1} is known only to Bob.

Q:

Alice ⟷ Bob

$f_1()$ ← private key, $f_1^{-1}()$ ← public key

Oscar

Bob private key ← $f_2()$, public key ← $f_2^{-1}()$

Alice has to prove his identity (Authentication)

Oscar shouldn't know the message (confidentiality)

Oscar shouldn't tamper the message.

Alice:

$m \Rightarrow f_1^{-1}(h(m))$ — x — y — m

c

sends $f_2(f_1^{-1}(h(m)))$ — $f_2(m)$

Bob verifies

$f_1(f_2^{-1}(x)) = h(f_2^{-1}(y))$

$f_1(f_2^{-1}(x)) = h(f_2^{-1}(y))$

$f_2(f_1^{-1}(h(m)))$, $f_2(m)$ → message cannot be decrypted

Can only be decrypted by Bob only

$f_1^{-1}(h(m))$ to m

Shows Alice's Authenticity

- First key can be shared through this process then after we can use E and D functions.

Public Key Certificate

- Tieing a person to his/her physical identity to virtual (digital) identity

~~1.~~ physical identity → virtual identity

Ex: passport (Issued by Govt of India)

- public key can be a potential digital identity.

Browser works on public key.

Client Alice ⟷ Server Bob.

(Has to prove his Identity to Alice).

- Need Digital certificate.

Digital identity = public function f
= (embedded public key)

Solution is PKI - Public Key Infrastructure.

- all about public key certificate

public key ≠ public key certificate.

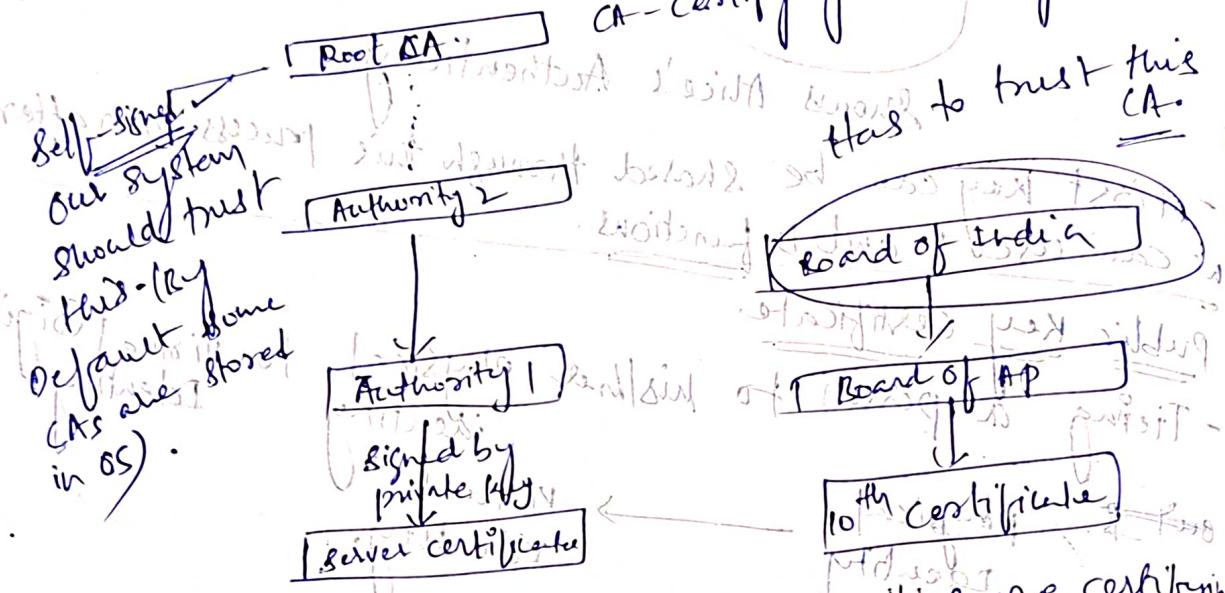
↓

Digital Identity.

How can we trust any website?
Every server should have a certificate.

Browser gives validation of Digital certificate. we can trust our browser
↓
Has a program to validate.

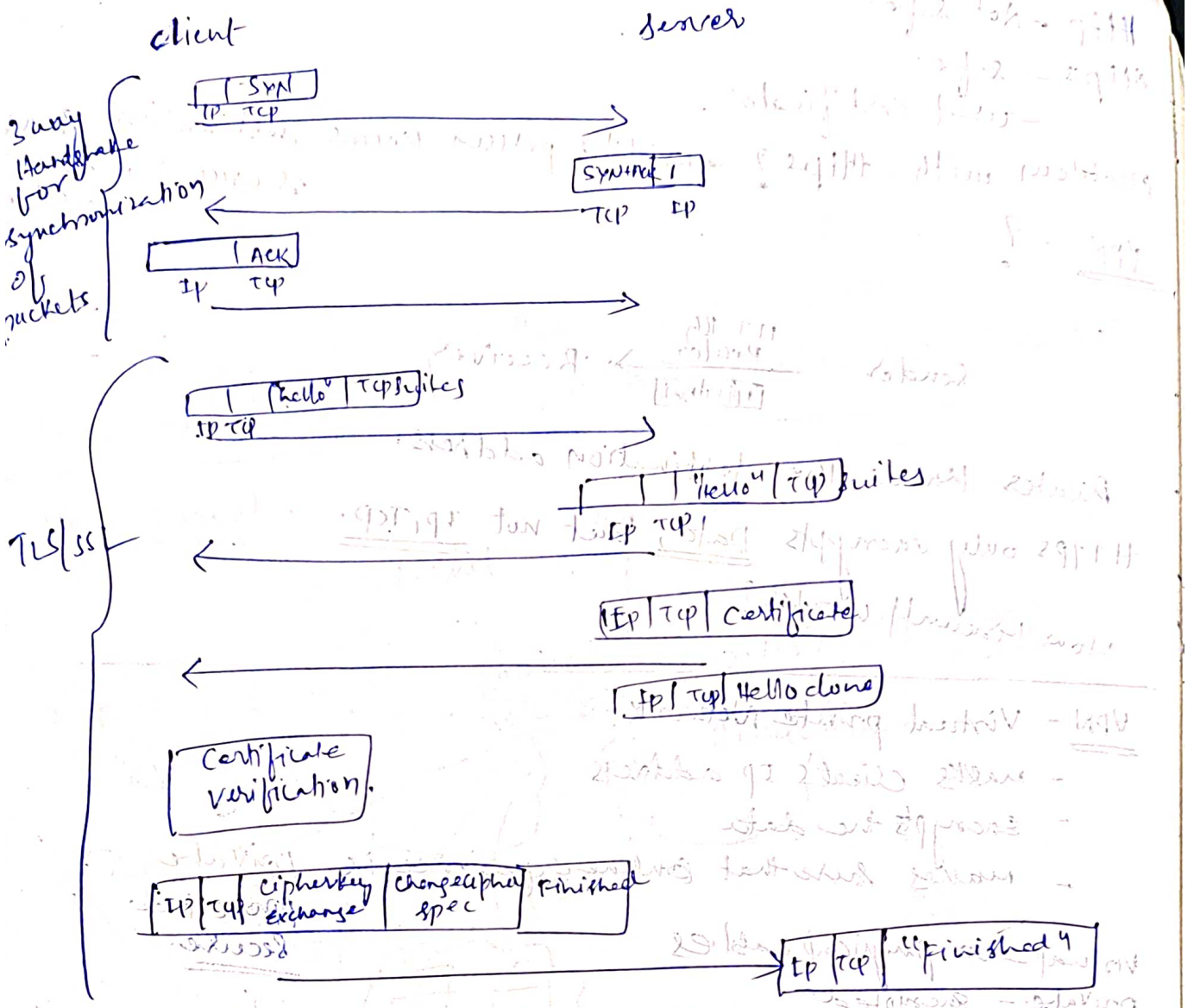
Chain of Trust:



How we can confirm that original Authorities are certifying the certificates?
A) As we are decrypting certificates with public key of original certificates then if correct Authority encrypts then only we can decrypt it.

SSL - Secure Socket Layer
- provides Authenticity and privacy.
- Communication with 'trusted' sites.
- Digital certificates for authentication.
  ↓
  Binds public key to the identity of the private key owner.
- Authentication happens at Connection Time.

How a connection Established?
- An SSL Connection is established through a Handshake
  ↓
  A series of Communication Exchanges.
b/w client and Exchange



Cipherkey exchanged } - shares a random string (premaster secret), after decrypting which server can derive session key.

- client encrypts premaster secret with server's public key.

Change cipher spec - signals that client and server agreed upon the cryptographic parameters, ready to switch to newly negotiated cryptographic settings.

Finished - verifies integrity of Handshake - whether the data got tampered b/w.

- Finished by client and server are different, as Encryption algorithm introduces some randomness.

Http - Not Safe.
Https - Safe.
- used certificates.

problem with Https? - Middle person knows destination server address.

VPN - ?

Sender → IIT Bh Router → Receiver

Router knows the destination address.

HTTPS only encrypts Data, but not IP, TCP.

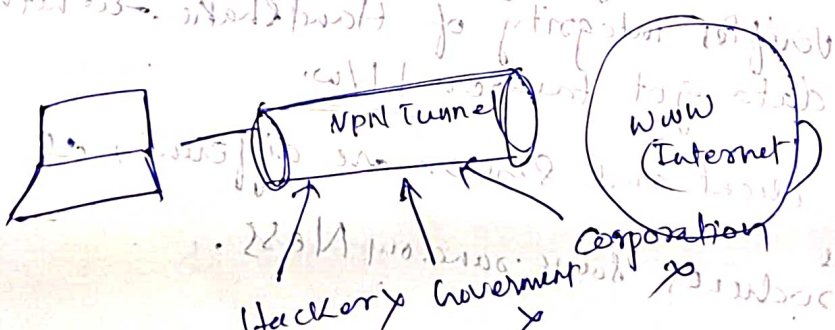
How Firewall works?

VPN - Virtual private Network.
- masks client's ip address
- encrypts the data
- makes sure that online experience is private protected secure.

Virtual - No physical cables
private - encrypted
Networked - ~~works on mail~~ multiple devices - computer and server work together.

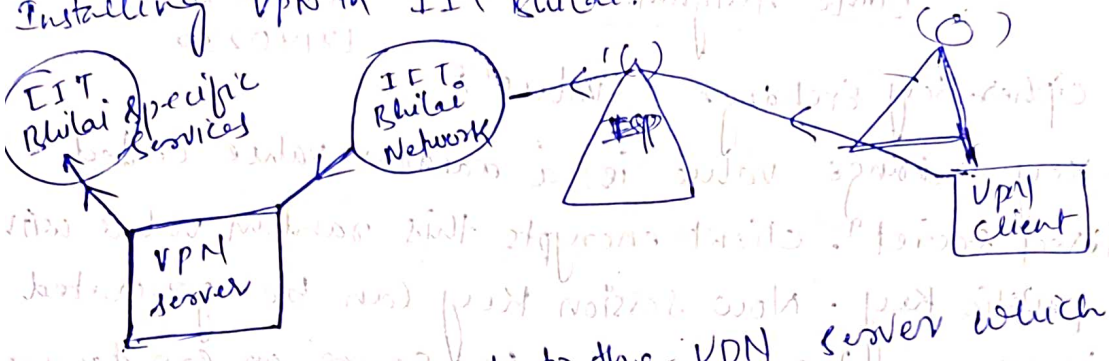
- provides anonymity ⇒ privacy.
- greater freedom for those who wish to access blocked or region bound content.

HTTPS also encrypts data? Then why VPN?
A) HTTPS won't protect your entire device. Just encrypts data b/w Browser and website while VPN encrypts all data in all the apps like: GMail, File downloads etc.)



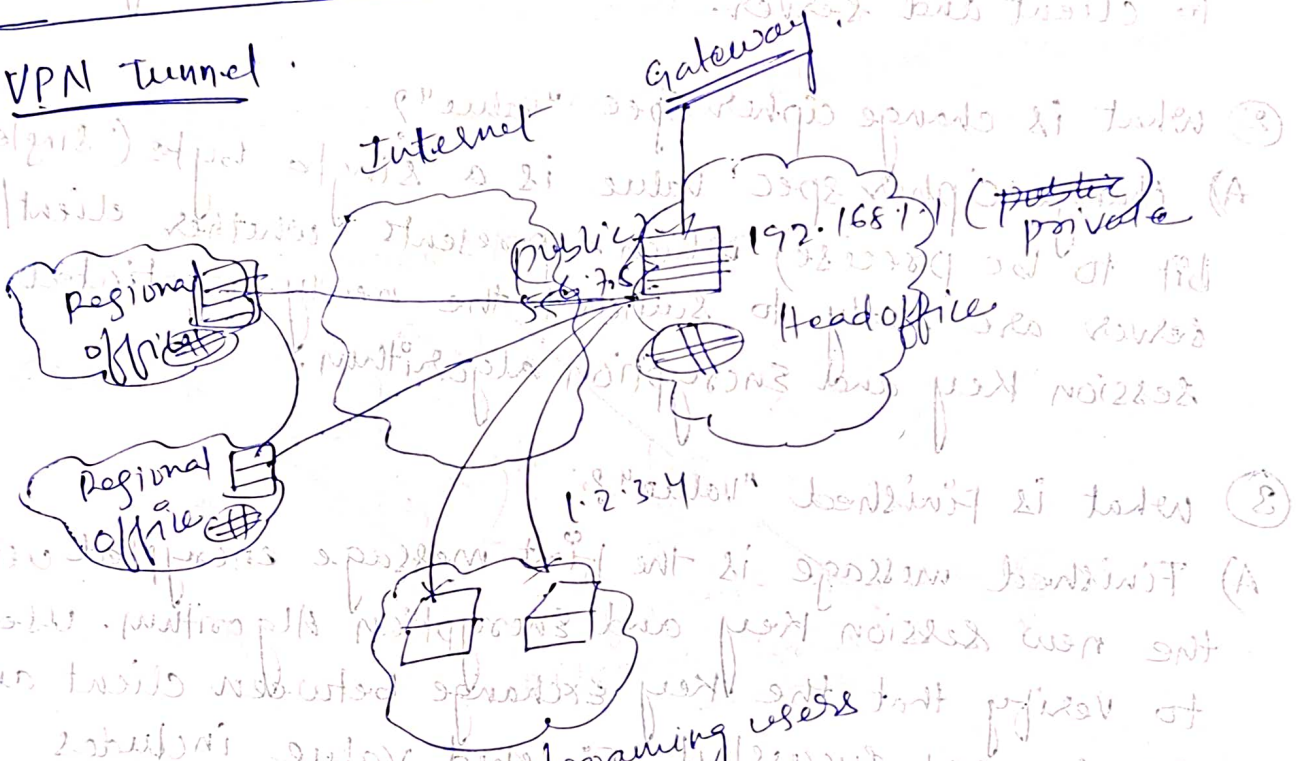
Https + VPN = Deadly combo ⇒ forms perfect team.

Installing VPN in IIT Bhilai.



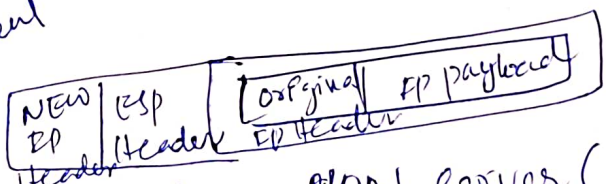
VPN client connects to the VPN server which is hosted in IIT Bhilai and having I.P address related to IIT Bhilai.

VPN Tunnel.



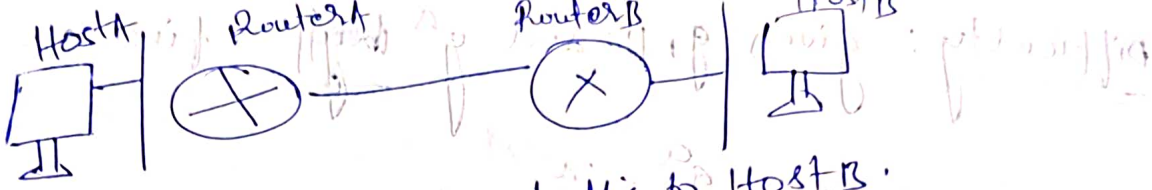
VPN verifies whether 1.2.3.4 is a legitimate user.
Normal gateway verifies 4.
VPN server - VPN gateway.
VPN client - running in client machine.

By VPN client



NEW IP destination - VPN server (5.6.7.8)
- decrypt it - Finds original destination

Ipsec - site to site protocol.



1. HostA sends interesting traffic to HostB.
2. RouterA and RouterB negotiate on IKE phase one session.

IKE – Internet Key Exchange.

IKE SA ⟷ (IKE phase1) IKE SA

3. phase 2 session establishment
* 4. Information is exchanged via IPSec Tunnel.

DH – Diffie Hellmann Key Exchange.

Given g^a, g^b;

$g^{ab} = (g^a)^b \Rightarrow (g^b)^a$

Given g, g^a, it is difficult to find a ⇒ Discrete Algorithm

Interested traffic – traffic that need to be protected by IPSec.

DH Key exchange

Alice and Bob agrees on g and p.

Alice creates private key (a).

Calculates $g^a \bmod p$

Bob creates private key b.

Calculates $g^a \bmod p$

Computes $(g^b \bmod p)^a \bmod p$
$= g^{ba} \bmod p$

$(g^a \bmod p)^b \bmod p$
$= g^{ab} \bmod p$

Difficulty: given g, p and $g^a \bmod p$, find a.

$g^a = x$

$a = \log_g x$

$(g^0, g^1, g^2 \ldots g^{n-1})$

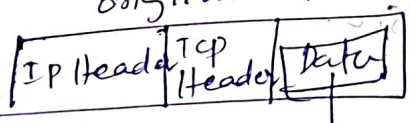
Ipsec - protocol used in VPN
- VPN Ipsec (VPN SSL can also be used)
VPN cisco.

IP packet converted into Ipsec packet. How?
↓
Various modes.

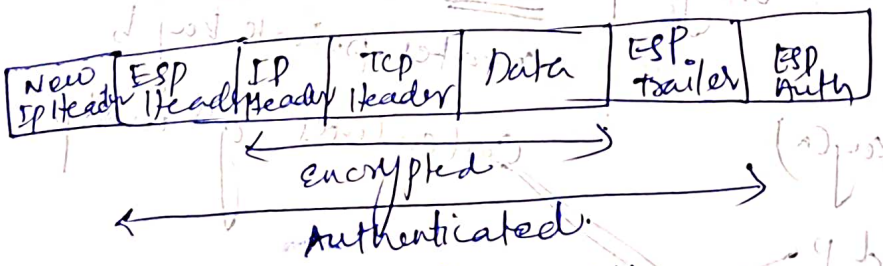
Ipsec in ESP (Encapsulating security payload) Tunnel mode
↓
Guarantees Authenticity and privacy.

HTTP - No security
HTTPS - some sort of Authentication
VPN - High level Authentication, privacy, Integrity.

original IP packet



↓
In HTTPS this is encrypted



- An intelligent person in middle can know whether the packet is TCP/ESP type.
↓
Can determine whether IP/Ipsec

SPI - Security parameter Index
= 32 bit (tells what sort of Algorithm they are using.)
Encoded in these Bits

Sequence Number

What is Next=IP ?
↓
IP protocol Not ESP

In TCP Header
proto = 6 ⇒ TCP protocol

HMAC - Authentication Algorithm
- Hash with Key
- If any Bit in the Encrypted packet changes ICV can figure it out.

- Router-Router VPN until Now

Site-Site VPN:

Remote Access VPN

SSL VPN ?

Site-site = Router-router = gateway-gateway (Key is shared physically)

Remote Access VPN

SSL VPN - (use certificates of origin Authentication)

- All of the three above VPN types differ from origin/identity Authentication.

Data Authentication ≠ origin Authentication.
↓
Anyone can know data but how to identify correct person

Gateway - entry point Router of any Network.