Unit 2

IP Security (IPsec)

It is an IETF Standard between two communication points across the IP network that provide data, authentication, integrity & confidentiality

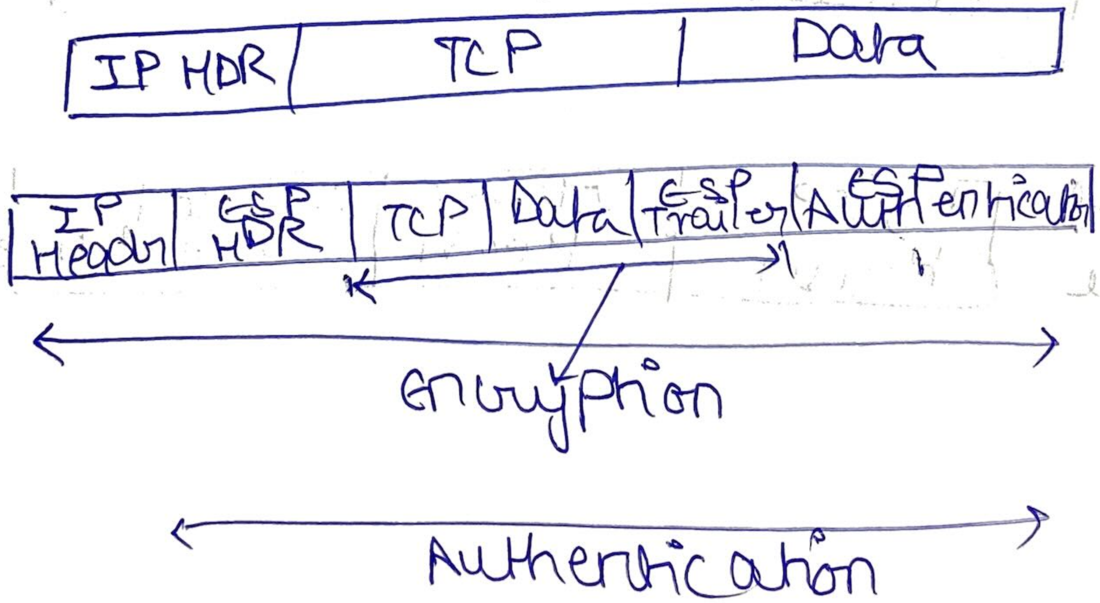
* Data Authentication (Identity validation)

* Integrity (Data/Info should be real/original)

* Confidentiality (Privacy)

Components of IP Security

1) Encapsulating Security Payload (ESP)



2) Authentication Header

IP Header	AH	TCP	Data

3) Inrurnet Key Exchange

→ It provides message contained protection by dynamically exchange encryption key

Two Phases

→ Phase 1

→ Phase 2

IPsec Turnel & Transport Mode

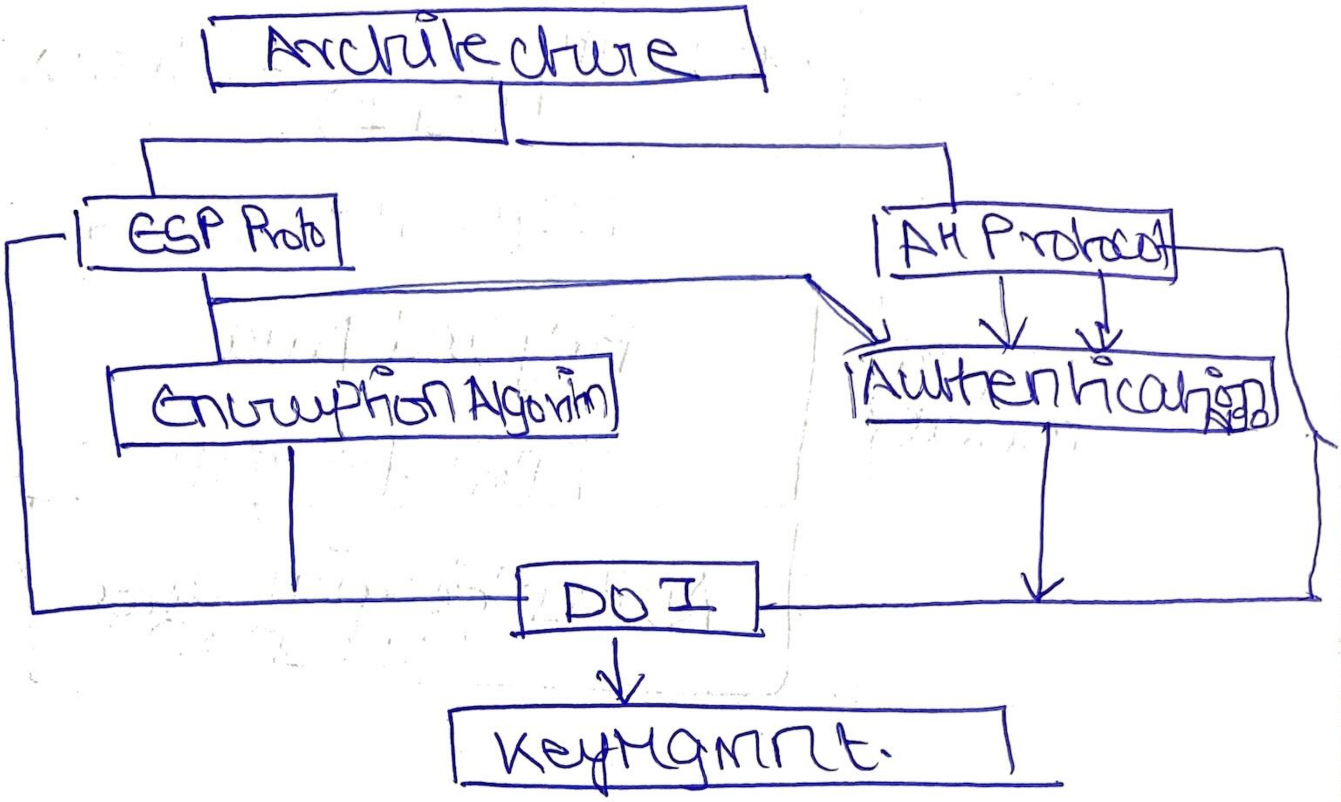
Transport Mode

original IP Header	IPsec Header	Protected Packet Data Field

Turnel Mode

No IP Header	IPsec Header	Protected original Packet

IPSecurity Architecture



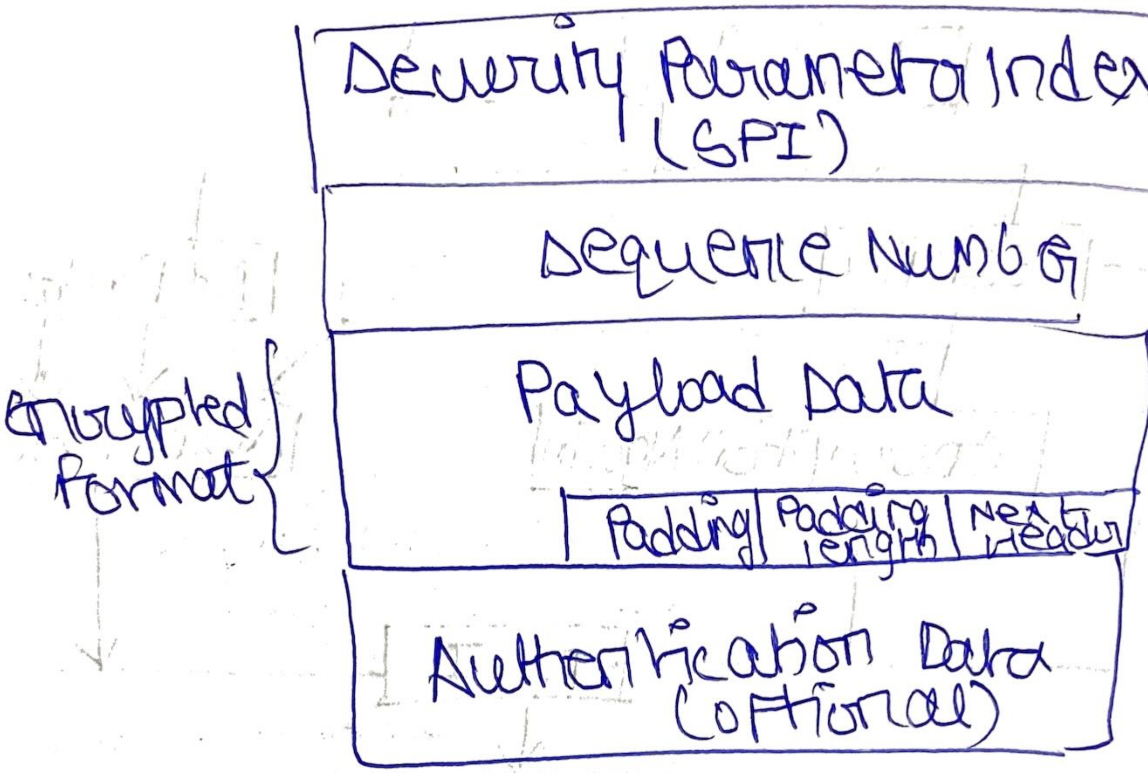
→ It covers the general concept protocols, definitions, algorithms & sec requirments of IP technology

→ ESP Protocol.

These are ~~the~~ implemented in two ways:

1) ESP with optional authentication

2) ESP with Authentication.


Security Parameter Index (SPI)
Sequence Number
Payload Data
Padding
Padding length
Next header
Authentication Data (optional)
Encrypted Format

unit3

Security services over E-mail

1) Privacy
2) Authentication
3) Integrity
4) Non Repudiation (Recipient proves that the sender sent it)

5) Proof of Submission
6) Proof of Delivery
7) Message flow confidentiality (Eavesdropper cannot determine the server ID)

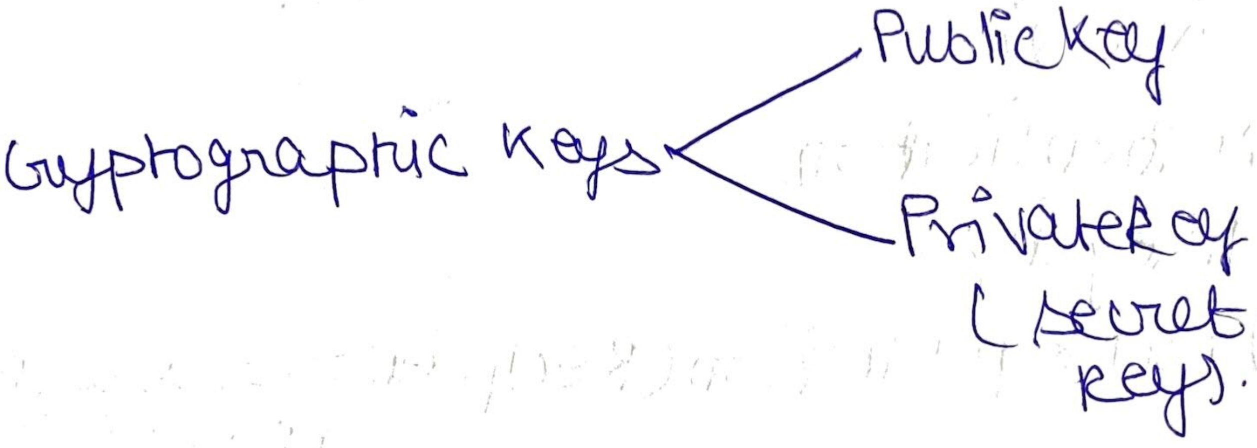
8) Anonymity (Ability to send so that the recipient does not know sender)

9) Containment (Secure Message with a region)

10) Audit (logging of events)
11) Accounting(night changes for server

12) Self Destruct
13) Message sequence integrity.

Establishing keys

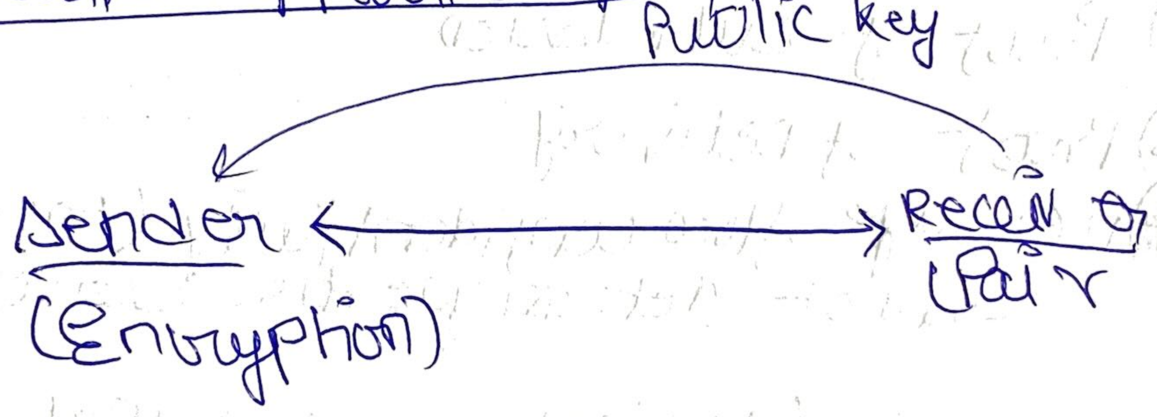


Cryptographic keys

Public key

Private key (secret keys).

I. Establishing public keys



Public key

Sender (Encryption)

Receiver (Pair)

- → Receiver may be appended in
- → Receiver may have certified through a C
- → Receiver may have hosted it on a PKI. (Public Key Infrastructure).

II Establishing private key

a) Both Parties meet in private to set a key

b) Communicate on the phone.

c) senders gets a ticket from KDC (key Distribution centre).

PGP (Pretty Good Privacy)

→ PGP is a open software for email security. It provides privacy, integrity, authentication and non repudiation

→ It also provides compression by using ZIP algorithm & the radix 64 encoding scheme.