Unit-3

Email privacy:

* **PGP (Pretty good privacy):**

Email privacy: It is defined as steps taken to protect your emails from being read by unauthorized or unintended recipients. The PGP is a technique used to achieve email Security. Service provided by PGP are authentication, Confidentiality, digital Signature.

PGP:

M - Message

EP - Encopting the hash function

H - hash function (mathematical function applied for not to modify data)

PRA - private key (A Sender)

P - Plain text (combination of message and encrypted hash function)

Z - Zipping the file (Compressing text)

R - Recrever Side

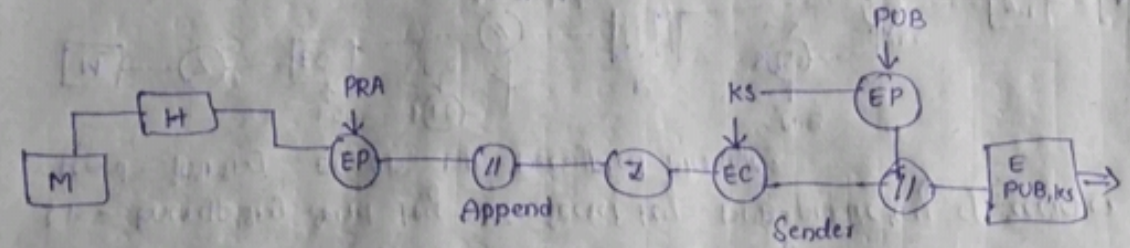
Z' - unzip (uncompressing the file)

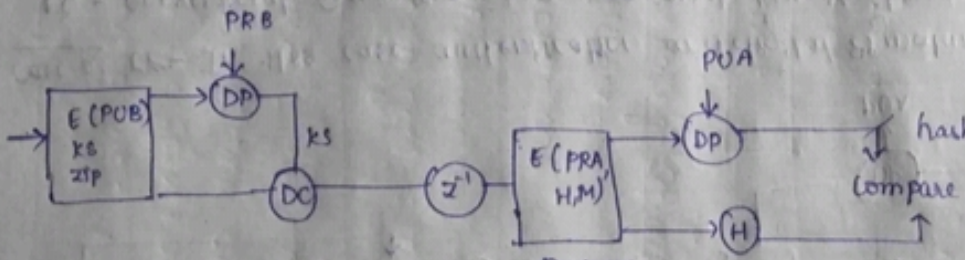
E(PRAH) - Private key of A, H encryption

DP - Decrypted plain text

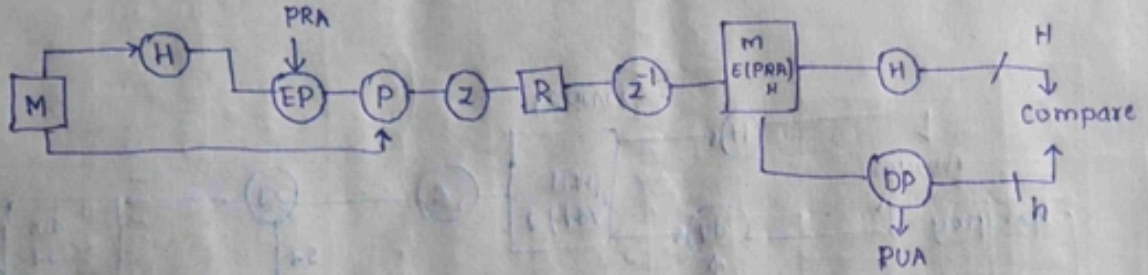
compare of Dp and H.

Case-3: we Can achieve Confidentiality, authentication, digital Signature. (case1 + case2)





Case-1: In Case 1 there is no Confidentiality but authentication and digital Signature is achieved

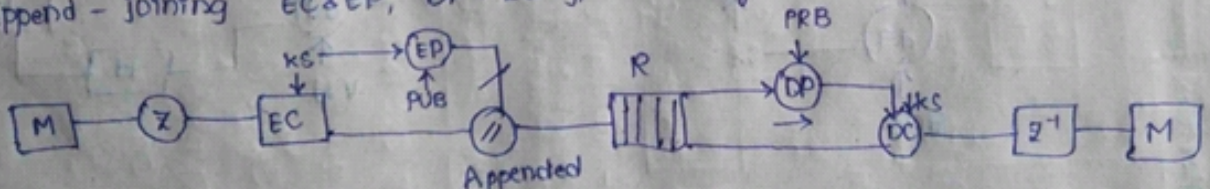


Case-2: ~~EC~~ In this case authentication and digital Signature is not achieved

EC - Conventional Encryption where same secret key is shared b/w Sender and reciever

EP - Encrypting Secret key KS - Secret key PUB - public key of reciever

append - joining EC & EP, DP - Decrypted Message.



~~Units~~

* S/MIME (Multipurpose Internet Mail extension).

↓

Security

→ The emails in previous days are sent in ASCII format. where audio, vedio, images could not be sent.

→ Using MIME we are allowed to transfer audio, video. images in email.

→ The extension of MIME is S/MIME. where S indicates with security.

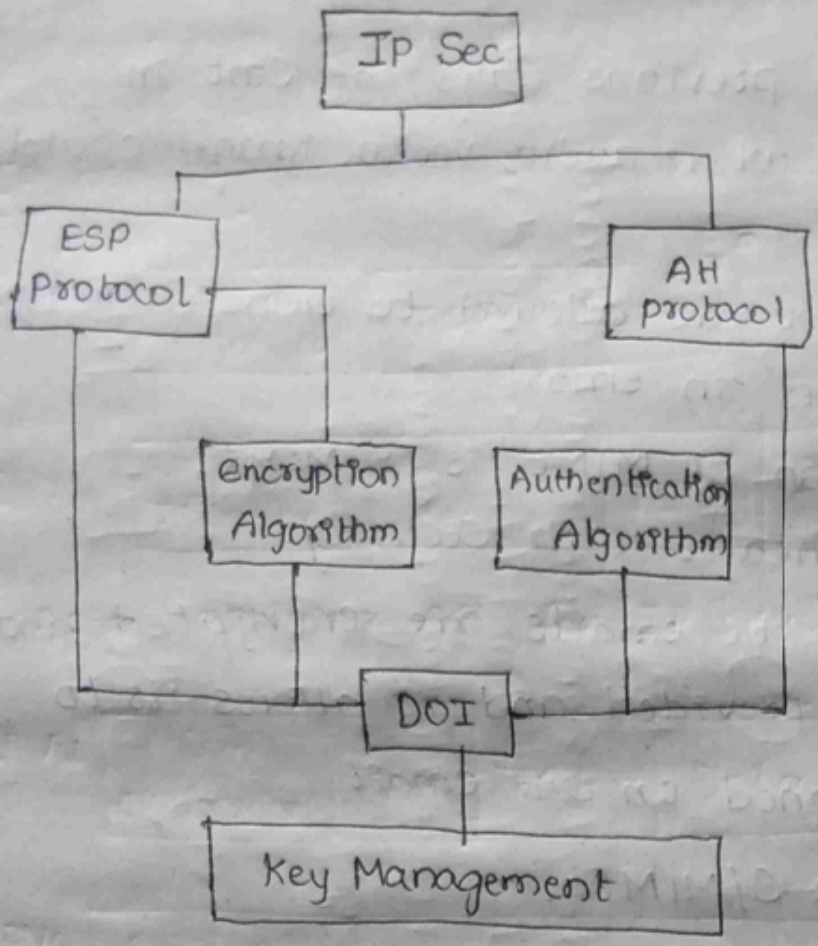
→ In S/MIME the emails are encrypted and Security is provided and it allows us to digitally signed on our email.

→ Functions of S/MIME :

1. Authentication.
2. Message integrity.
3. Non-repudation (no denail)
4. privacy.
5. Data Security.

* IP Security :-

Architecture or block diagram :



ESP Stands for Encapsulating Security protocol.

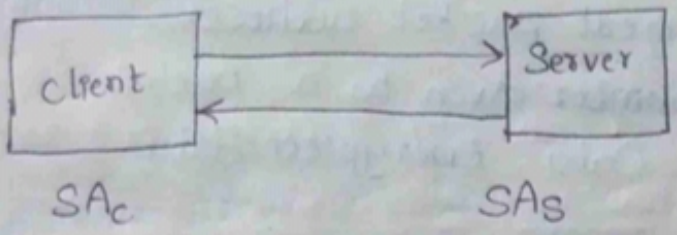
AH - Authentication Header.

DOI- Domain of Interpretation

* Security Association (SA)

→ In IP Security the main goal is to achieve security association.

→ The Security association is one way communication where at a time only client can send message to the server or Server can send message to client.



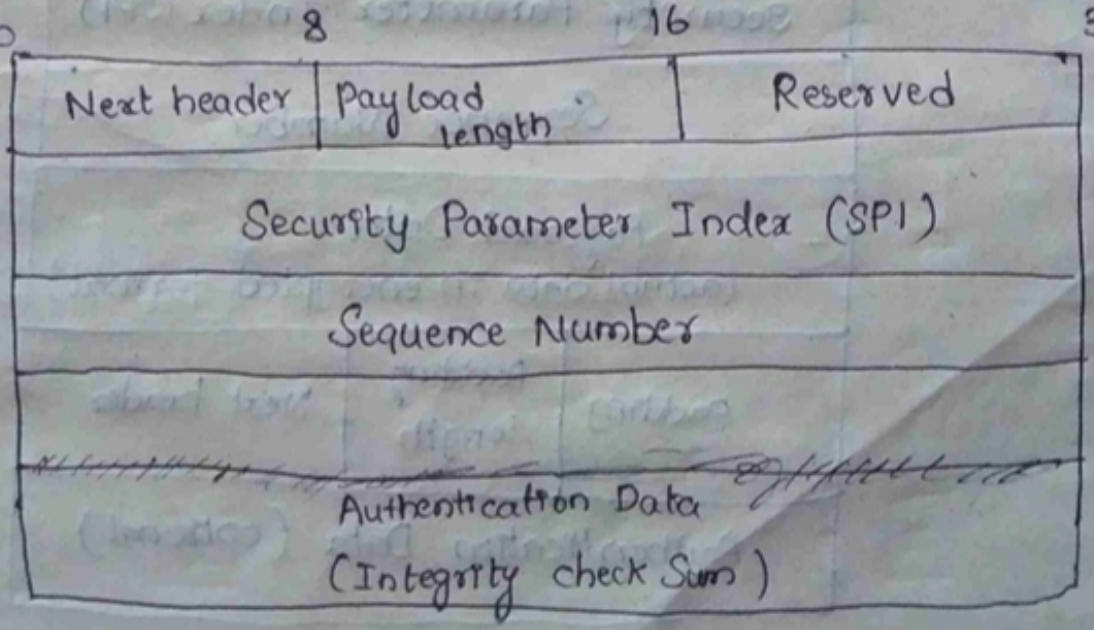
One way communication.

* Parameters of Security Association (SA):-

1) Security parameter Index (SPI)
2) Sequence Number Counter
3) Sequence Number Overflow
4) Anti-Replay window
5) AH information.
6) ESP information
7) Life time of SA.
8) IP Security protocol mode < Transport / Tunnel

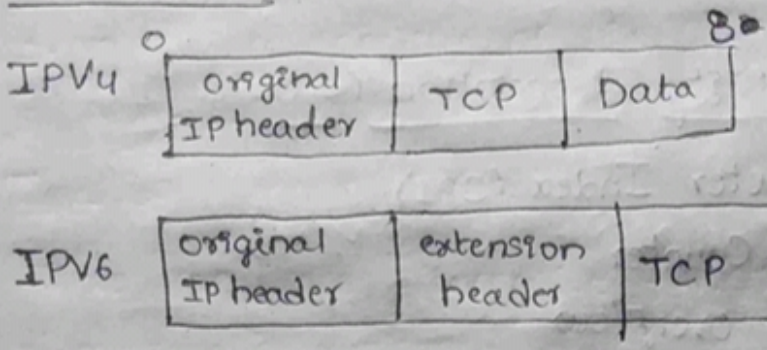
* Authentication Header (AH):-

In this authentication header we need to achieve authentication along with integrity Following is a packet format:

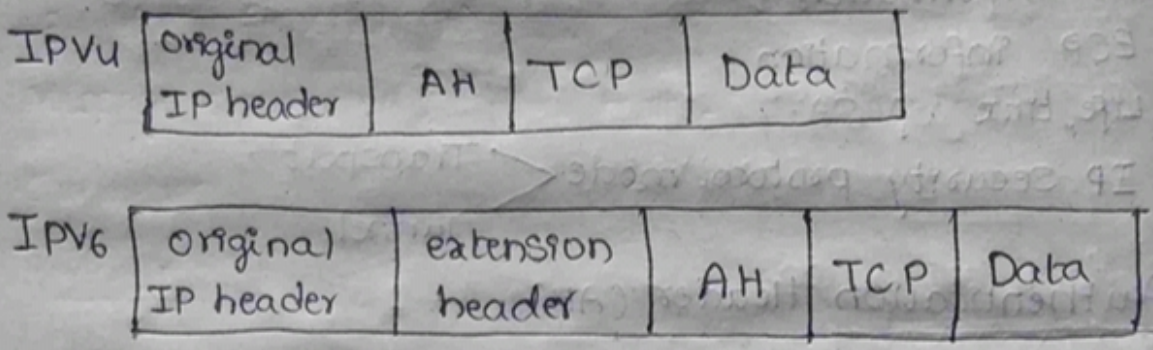


Next header : next packet address
SPI : Unique number given to a packet
Authentication Data : Encrypted data.

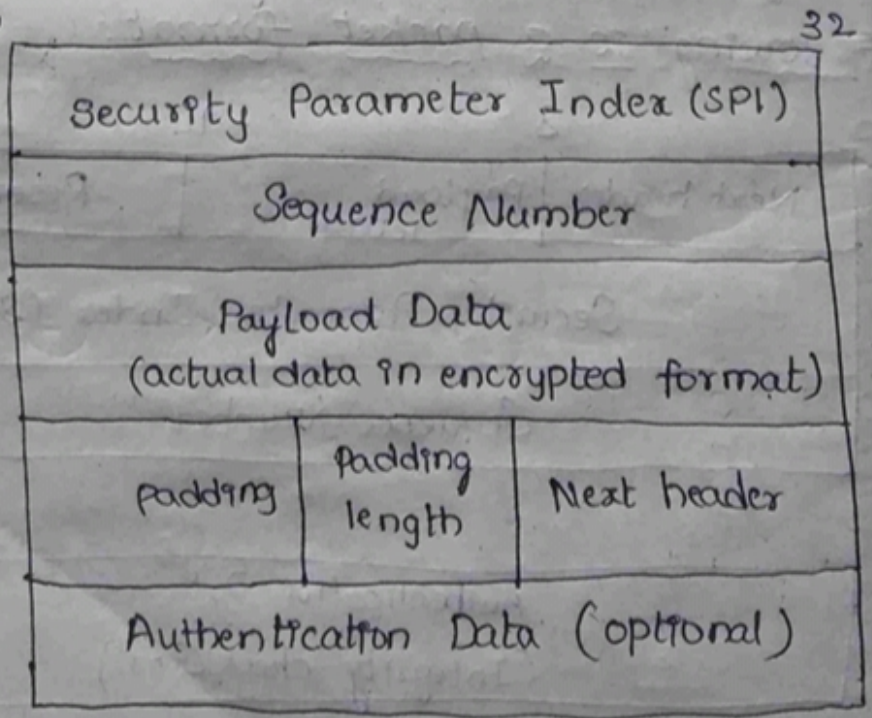
* IP header :



After applying AH for IP header



* ESP Packet format :-



padding : adding with dummy bits.

* IP Headers :

IPV4

original header	TCP	Data

IPV6

original IP-header	extension headers	TCP	Data

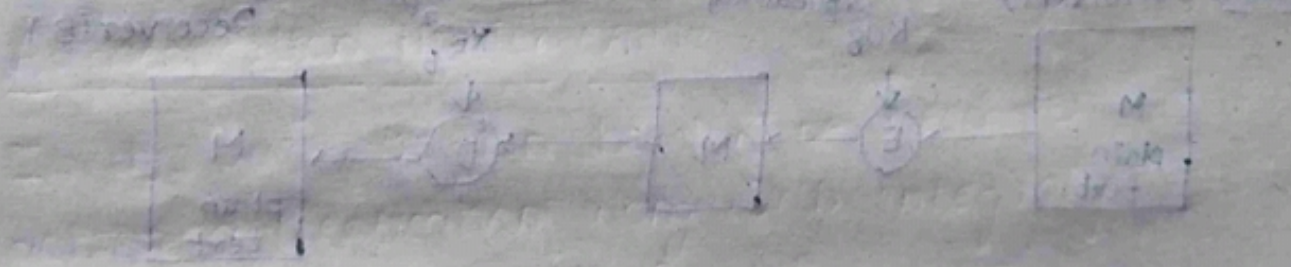
Applying ESP to IP headers

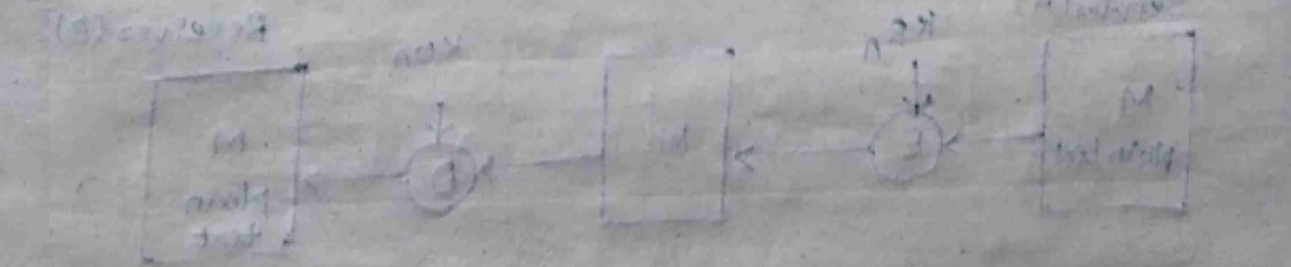
IPV4

original IP header	ESP header	TCP	Data	ESP trilar	ESP Authen-tication

IPV6

original IP header	extension header	ESP header	TCP	Data	ESP trilar	ESP Authenti cation





* Internet key Exchange (IKE):

It is a secure key management protocol used to setup a secure communication b/w two devices.

The IKE is done in two ways

1. manual
2. Automated.

* Manual: In manually it configures each system which is small and static.
* Automated: It is done on demand creation of keys for large and distributed systems.

In automated there are two protocols

1. Oakley key determination protocol
2. ISAKMP [Internet Security association key management protocol.

Oakley key determination protocol:

It is based on diffie hellman key exchange protocol with added security, generic protocol.

ISAKMP:

It provides a framework for key exchange and provides protocol specific support.

IKE is done in two phases phase1 and phase2

phase-1:

The exchange of proposals for Security Services where encryption and decryption algorithms are used when both ends of tunnels are agree to accept a set of Security parameters then phase1 is completed.

phase-2:

Once participation is established a Secured channel in phase 1 they move to phase 2 here Security associations are negotiated, which decide to use ~~the~~ AH by ESP and also select with algorithm to use and phase 2 always Operates in Quick mode.