4 Authentication & Digital ~~Signature~~

Page No :
Date :

* PGP (Pretty Good Privacy.)

i) It is a remarkable phenomenon.
ii) Developed by Zimmermann.
iii) PGP provides a confidentiality & authentication service that can be used for electronic mail & file storage application.
iv)

Zimmermann has done the following /

1) selected best available cryptographic algo. as building blocks.
2) Integrated these algo. into general purpose application that is independent of os & processor & i.e based on small set of easy to use commands.
3) Made package & its documentation, including the source code, freely available via Internet, bulletin boards & commercial nlw such as AOL
4) Entered into an agreement with company to provide a fully compatible, low cost commercial version of PGP

* PGP has grown explosively & is now widely used.

1) It is available free worldwide in versions that on variety of platforms, including windows, Unix.
2) It is based on algo. that have survived extensive public review & considered extremely secure.
3) PGP is now on an Internet std. track. PGP still has an aura of an antiestablishment endeavor.

Notation

The following symbols

Ks = Session Key used in symmetric encryption scheme
PRa = Private Key of user A
PUa = Public Key of user A
EP = Public Key Encryption
DP = Public Key decryption
EC = symmetric encryption
DC = symmetric decryption
H = hash fun.
|| = concatenation
Z = compression using ZIP alg.
R64 = conversion to radix 64 ASCII format

Sulekha

Operational Description

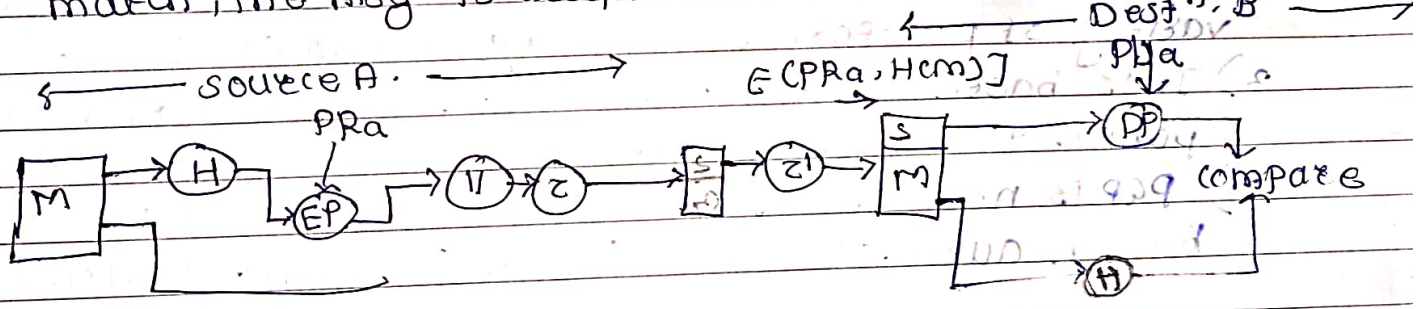
The actual operation of PGP as opposed to the mgmt of keys, consists of five services

a) authentication
b) confidentiality
c) compression
d) email compatibility
e) segmentation.

Authentication

The digital signature service provided by PGP. The sequence is as follows.

1) The sender creates a message.
2) SHA-1 is used to generate a 160 bit hash code of the msg.
3) The hash code is encrypted with RSA using the sender's private key & the result is prepended to the msg.
4) The receiver uses RSA with the sender's public key to decrypt & recover the hash code.
5) The receiver generates a new hash code for the msg. compares it with the decrypted hash code. If the two match, the msg. is accepted as authentic.



Confidentiality

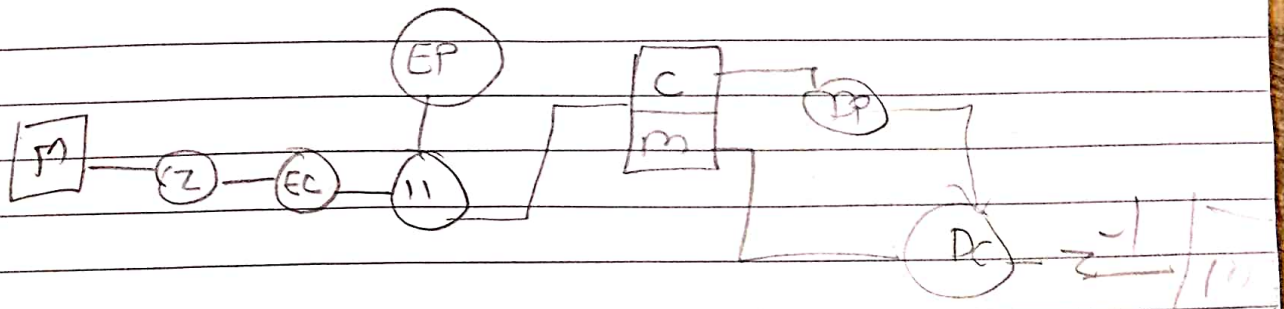
-Another basic service provided by PGP is confidentiality which is provided by encrypting msg. to be transmitted or to be stored locally as files.
- In both symmetric encryption algo. CAST-128 may be used.

1) The sender generates a msg. & random 128 bit no. to be used as session key for this msg. only.
2) The msg. is encrypted using CAST-128 with session key.
3) The session key is encrypted with RSA using the recipient's public key & is prepended to the msg.

Date :

4) The receiver uses RSA with its private key to decrypt & recover the session key.

5) The session key used to decrypt the msg.

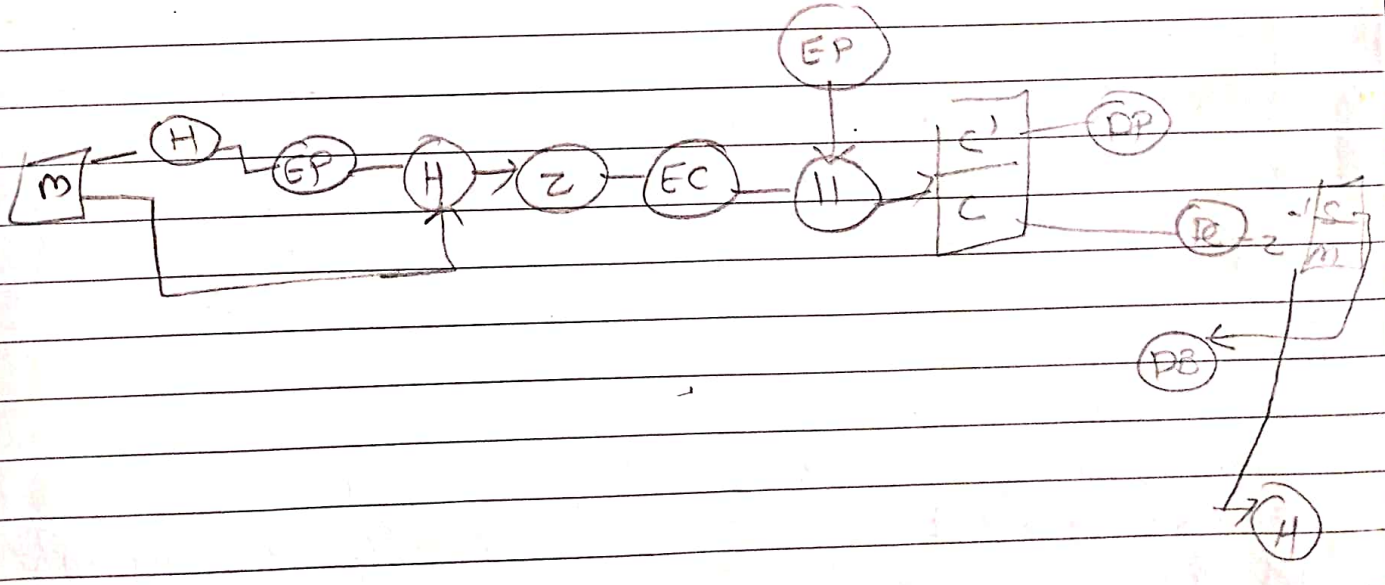


- confidentiality & Authentication

i) Both services may be used for the same msg.

ii) First signature is generated for the plaintext msg. & prepended to the msg.

iii) Then plaintext msg plus signature is encrypted.



Page No:
Date:

S/MIME (Secure/Multipurpose Internet mail Extension)

i) It is a security enhancement to the MIME internet email format standard, based on technology from RSA data security

MIME

i) It is an extension to the RFC 822 framework that is intended to address some of the problems & limitations of the use of SMTP or some other mail transfer protocol & RFC822 for electronic mail

Limitations

1) SMTP can't transmit executable files or other binary objects. A no. of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems, including the popular UNIX UUencode/UUdecode scheme. However none of these is std. or even de facto std.

2) SMTP can't transmit text data that includes national lang. characters because these are represented by 8 bit codes with values of 128 decimal or higher & SMTP is limited to 7 bit ASCII

3) SMTP servers may reject mail message over certain size.

4) SMTP gateways that translate bet. ASCII & character code EBCDIC don't use consistent set of mappings resulting in translation problems.

5) SMTP gateways to X.400 email nw can't handle nontextual data included in X.400 msg.

6) some SMTP implementation do not adhere completely to the SMTP std. defined in RFC 821

Sulekha

Overview

The MIME specification includes the following elements

1) 5 new msg. header fields are defined which may be included in RFC 822 header. These fields provide info. about the body of msg.
2) A no. of content formats are defined, thus standardizing representations that support multimedia email
3) Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by mail system.

The five header fields defined in MIME

1) MIME version
Must have the parameter value 1.0. This field indicates that the msg. conforms to RFCs 2045 & 2046.
2) Content type
Describes the data contained in the body with sufficient detail that receiving user agent can pick an appropriate agent or mechanism to represent data to the user or otherwise deal with data in an appropriate manner
3) Content-transfer encoding
Indicates the type of transformation that has been used to represent the body of msg. in a way that is acceptable for mail transport.
4) Content ID
Used to identify MIME entities uniquely in multiple contexts.
5) Content Description
A text description of the object with the body, this is useful when the object is not readable (e.g audio data)

MIME content types

i) Text → plain, enriched
ii) Multipart → Mixed, parallel, alternative, Digest
iii) Message → rfc822, partial, external body
iv) Image → JPeg, gif
v) video → mpeg
vi) Audio → basic
viii) Appln - postscript
octet stream

Page No :
Date :

S/MIME functionality

1) It is very similar to PGP, both offer the ability to sign & or encrypt messages. In this subsection, we briefly summarizes S/MIME capability.

1) Enveloped data
This consists of encrypted content of any type & encrypted content. encryption keys for one/more recipients.

2) Signed data →
A digital signature is formed by taking the msg. digest of the content to be signed & then encrypting that with the private key of signer. The content + signature are then encoded using base 64 encoding
A signed data msg. can only be viewed by recipient with S/MIME capability.

3) Clear signed data
As with signed data ds of the content is formed. However in this case only DS is encoded using base 64. As result recipients without S/MIME capability can view the msg. content, although they can't verify the signature

4) Signed & enveloped data
Signed only & encrypted only entities may be nested. so that encrypted data may be signed & signed data or clear signed data may be encrypted.

* IP security

Appln of IPsec
It provides capability to secure comm.n across a LAN, across private & public WANs & across the internet

1) Secure branch office connectivity over the Internet
A company can build a secure virtual private network over the internet or over a public WAN.

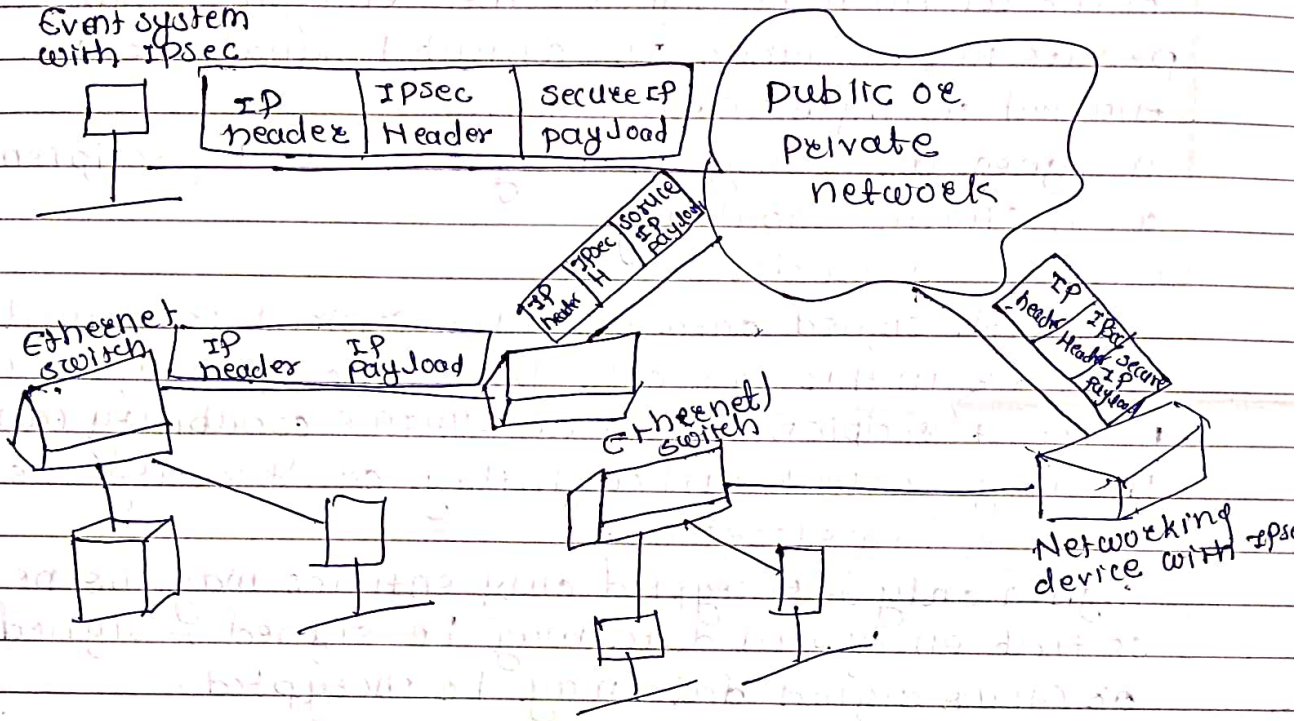
2) Secure remote access over the internet
An end user whose system is equipped with IP security protocols can make a local call to an internet service provider (ISP) & gain secure access to a company n/w. This reduces the cost of toll charges for travelling employees & telecommuters

3) Establishing extranet & intranet connectivity with partners

IPsec can be used to secure communication with other org., ensuring authentication & confidentiality & providing key exchange mechanism.

4) Enhancing electronic commerce security

Even though some web & electronic commerce appln ha built in security protocols, the use of IPsec enhances that security.



* Benefits of IPsec

1) When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

2) IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP & the firewall is the only means of entrance from the Internet into org.

3) IPsec is below the TCP, UDP & so is transparent to appln. there is no need to change s/w on user or server system when IPsec is implemented in the firewall / route

4) IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on per-user basis or revoke keying material when users leave the org.
5) IPsec can provide security for individual users if needed.

* IP Security Architecture

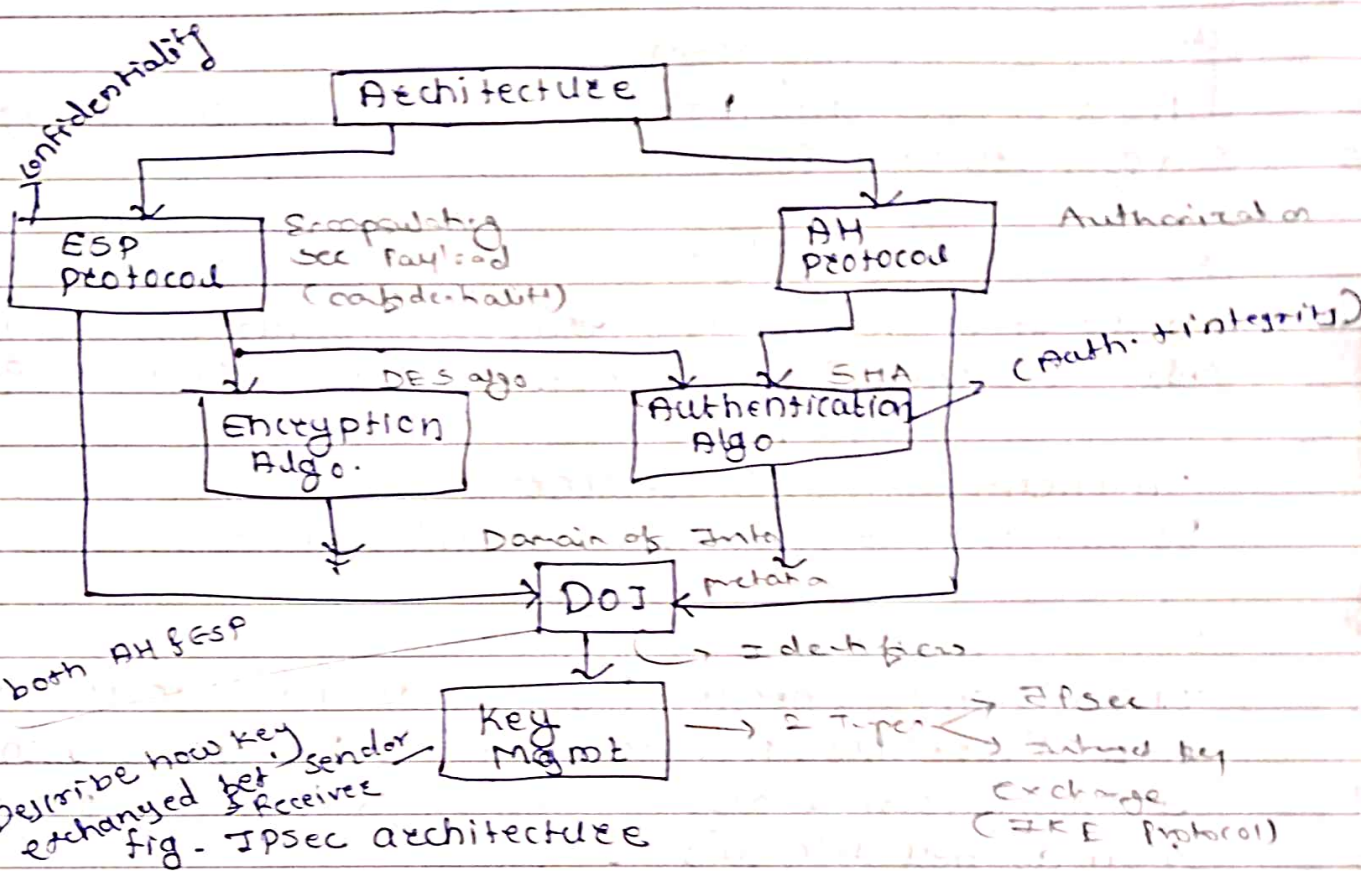


fig. IPsec architecture

i) In both IPv4 & IPv6 security features are implemented as extension headers that follow the main IP header.
ii) The extension header for authentication is known as the authentication header that for encryption is known as the ESP header

1) Architecture

Covers the general concepts, security requirements, definations & mechanisms defining IPsec technology.

2) Encapsulating security Payload (ESP)
covers the packet format & general issues related to the use of the ESP for packet encryption & optionally authentication.

3) Authentication Header (AH)
covers the packet format & general issues related to the use of AH for packet authentication.

4) Encryption Algorithm
A set of documents that describe how various encryption algo. are used for ESP.

5) Authentication Algorithms
A set of documents that describe how various authentication algo. are used for AH & for the authentication option of ESP.

- Authentica Key Management
Documents that describe key mgmt. schemes.

Domain of Interpretation (DOI)
contains values needed for other documents to relate to each other. These include identifies for approved encryption & authentication algo. as well as operational parameter such as key lifetime.

IP sec services
1) Access control
2) connectionless integrity
3) Data Origin authentication
4) Rejection of replayed packets
5) confidentiality
6) limited traffic flow confidentiality

	AH	ESP encry	ESP encry + auth.
Access control.	~	~	~
Connectionless integrity	~		~
Data origin authentication	~	~	~
Rejection of replayed packets	~	~	~
confidentiality		~	~
Limited traffic flow confidentiality			

Security Associations

i) An association is one way relationship bet^n sender & receiver that affords security services to the traffic carried on it.

ii) security association is uniquely identified by 3 parameters

1) Security parameters Index (SPI)
A bit string assigned to this SA & having local significance only. The SPI carried in AH & ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

2) IP destination Address
Only unicast addresses are allowed, this is the address of the dest. endpoint of the SA, which may be end user system or n/w system such as firewall

3) Security protocol Identifier
This indicates whether the association is an AH/ ESP security association.

SA parameters.

1) Sequence no. counter
A 32-bit value used to generate the sequence no-field in AH or ESP headers.

2) sequence counter overflow
A flag indicate whether overflow of the seq. no. counter should generate an auditable event & prevent further transmission of packets on this SA.

3) Anti-Replay window
Used to determine whether an inbound AH/ESP packet is replay.

4) AH information
Authentication algo., keys, key lifetimes & related para. being used in AH.

5) ESP info-
Encryption & authentication algo., keys, initialization values, key lifetimes & related parameters being used with ESP.

6) Lifetime of this SA
A time interval or byte count after which an SA must be replaced with new SA or terminated, plus an indication of which of these actions should occur.

7) IPsec Protocol Mode
Tunnel, transport, or wildcard.

8) Path MTU
Any observed path MTU aging variables.

* SA selectors
i) SA can be combined in no. of ways to yield the desired user configuration.
ii) IPsec provides a high degree of granularity in discriminating between traffic i.e afforded IPsec protection & traffic i.e allowed to bypass IPsec in the former case relating IP traffic to specific SAs
iii) The means by which IP traffic to specific SAs is the nominal Security Policy Database (SPD)
iv) SPD contains entries each of which defines subset of IP traffic & points to an SA for that traffic.

The following selectors determine an SPD entry.

1) Destination IP address
2) Source IP address
3) User ID
4) Data sensitivity level
5) Transport layer protocol
6) Source & Destination ports.

* Transport & Tunnel modes

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload & selected portions of IP header & IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header & outer IPv6 extension headers
ESP	Encrypts IP payload & any IPv6 extension headers following the ESP header	Encrypts entire inner IP packet
ESP with Authentication	Encrypts IP payload & any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	Encrypts entire inner IP packet. Authenticates inner IP packet.

* Authentication Header

AH consists of the following fields.

1) Next header (8 bits)
Identifies the type of header immediately following this header.

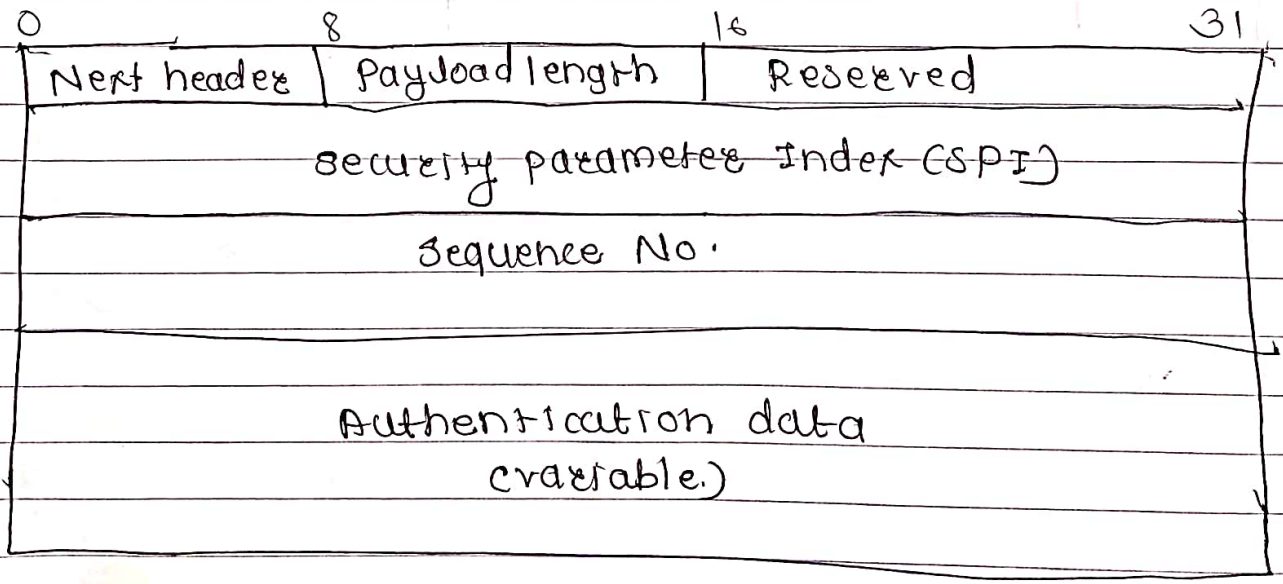
2) Payload length (8 bits)
Length of AH in 32-bit words, minus 2. e.g. the default length of the authentication data field is 96 bits or three 32-bit words with 3 word fixed header, there are a total of six words in the header & payload length field has value of 4.

3) Reserved (16 bits)

4) Security parameter Index (32 bits)
Identifies a security associations

5) Sequence No. (32 bits)
A monotonically increasing counter value

6) Authentication data
A variable length field that contains the integrity check value or MAC for this packet



Page No :
Date :

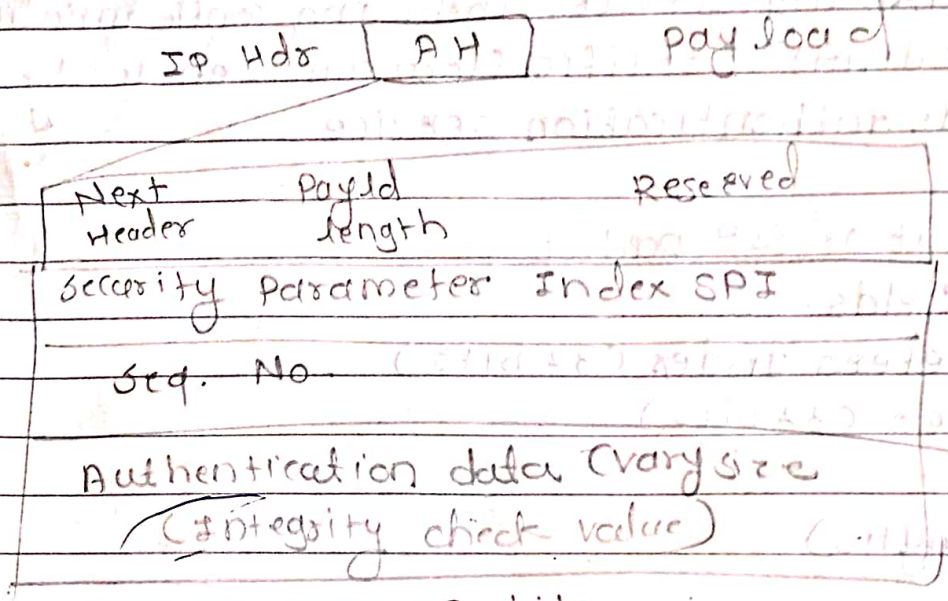
Encapsulating Security Payload

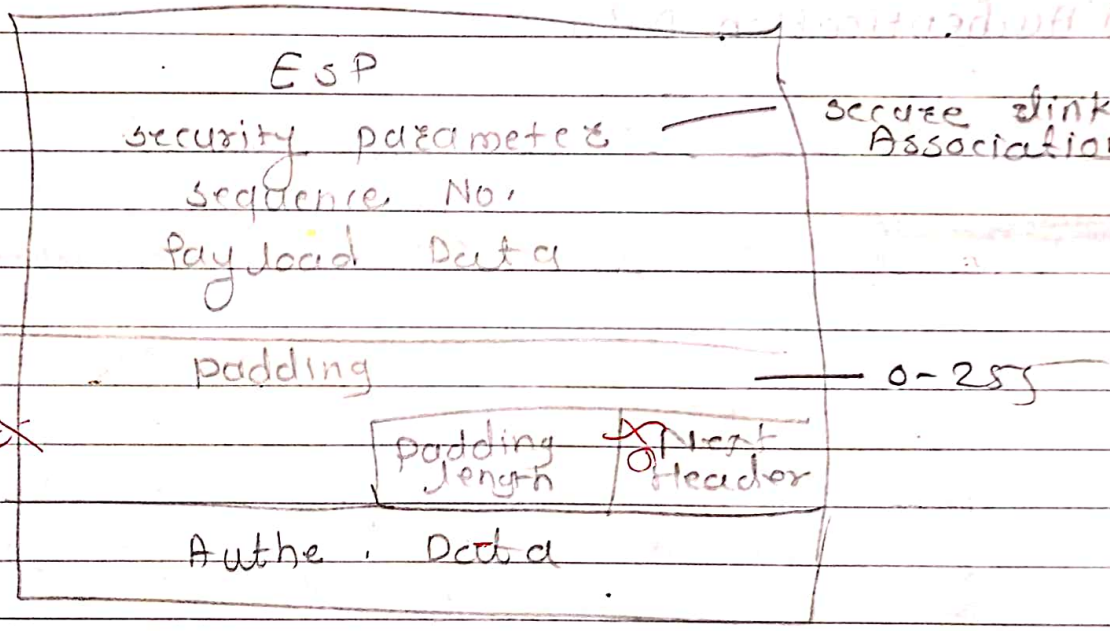
It provides confidentiality services, including confidentiality of msg. contents & limited traffic flow confidentiality ESP can also provide authentication service.

ESP Format - Format of ESP packet
It contains foll. fields.

1) Security parameters Index (32 bits)
2) Sequence number (32 bits)
3) Payload data.
4) Padding (0255 bytes)
5) Pad length
6) Next header 8 bits
7) Authentication Data.

AH


IP Hdr
AH
payload
Next Header
Payld length
Reserved
Security Parameter Index SPI
Seq. No
Authentication data (vary size
(Integrity check value)
32 bit


ESP
security parameters
Sequence No.
Payload Data
Padding
0-255
Padding length
Next Header
Authe. Data
Secure Links Association