Haste brings WASTE
Waste brings WORRY
Do not be in a HURRY

...Bhagwan Sri Sathya Sai Baba

Unit-5

Explain key management techniques in ISAKMP.

ISAKMP stands (Internet Security Association and Key Management protocol)

→ It provides a framework for establishing Security Associations (SAs) and cryptographic keys.

Key techniques:

1) Cookies:
   - used to avoid clogging attacks
   - Initiator & responder cookies unique identify each party

2) Authentication Methods:
   - used digital signatures, shared secret keys or public key encryption to authenticate both sides

3) Nonce Exchange:
   - random no's exchanged to prevent replay attacks

4) SA Negotiation
   - ISAKMP negotiates algorithms (AES/3DES), hash methods (SHA), key sizes & modes

5) Modular payloads
- SA payload
- key exchange payload
- Identification payload
- Authentication payload

These combineds to form a complete key exchange

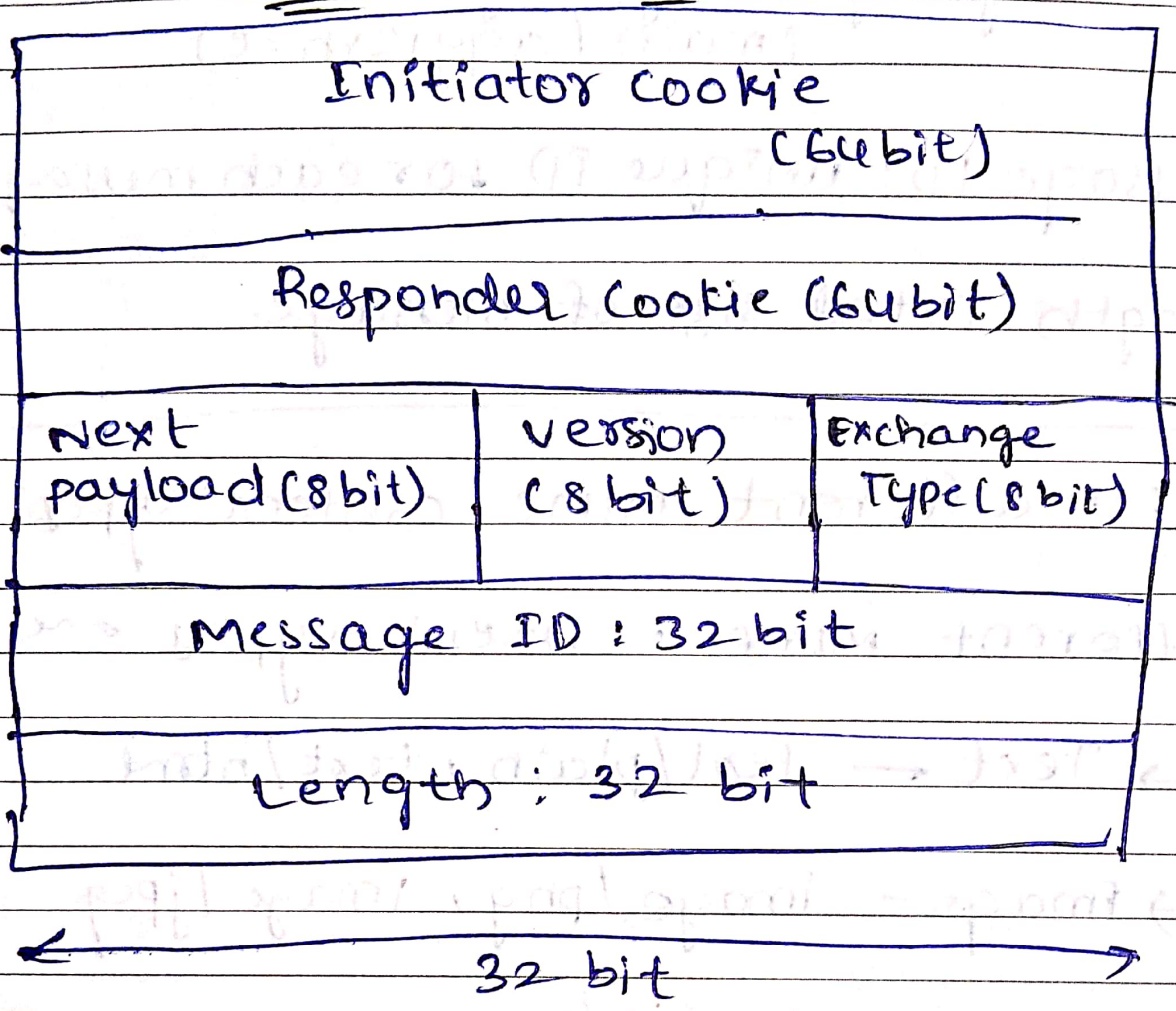
8) Specify documents in IPSec architecture:

Documents are

→ RFC 4301 - IPSec architecture
→ RFC 4302 - Authentication Header (AH)
→ RFC 4303 - Encapsulating Security Payload (ESP)
→ RFC 2408 - ISAKMP
→ RFC 2409 - IKE / Oakley
→ RFC 5996 - IKEv2

Draw ISAKMP frame structure & explain each field

ISAKMP structure



Fields :

- **Initiator cookie:** Identified the sender who starts the communication
- **Responder cookie:** Filled by responder (0 in first message)
- **Next payload:-** shows type of next payload (SA/KE/etc)

Version : ISAKMP version

exchange type : type of handshake (main / aggressive)

Message ID : unique ID for each message

length : Total size of message

Q) List different MIME content types?

different MIME content types are

→ Text — text/plain, text/html

→ Image — image/png, image/jpeg

→ Audio — audio/mpeg

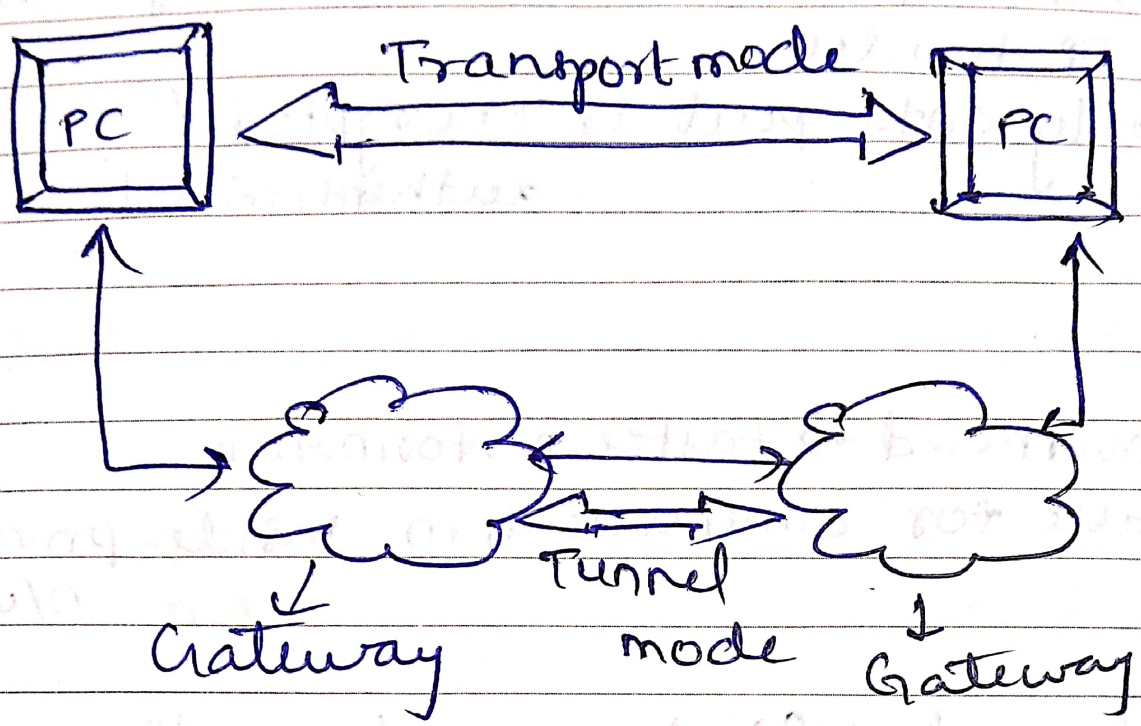
→ video — video / mp4

→ Application — application/pdf, application/zip

→ Multipart — multipart/mixed

→ Message — message/rfc822

Q Explain transport & tunnel modes of IPSec.



Transport mode (End-to-End Security)

→ It protects payload (data) of IP packet but does not protect the original IP header

→ used to Host-to-Host communication (eg b/w two computers)

→ used in remote login, file transfer, end-user machine security

How it works:

→ IP header stays unchanged
→ AH / ESP header is inserted after the IP header
→ only data part is encrypted / authenticated

Adv:

. less overhead → faster performance
. suitable for communication inside private n/w

Tunnel mode: (Gateway-to-Gateway Security)

→ protects the engire original IP packet, including IP header.
→ A new IP header is added outside
→ used in VPNs
→ used in Firewall communications

How to work:

. entire original packet is encapsulated & encrypted
. ~~Best for secure communication over the internet~~

. A new IP header is added to route the packet through the tunnel

Adv:

→ High security

→ Best for secure in communication

Q) Difference of transport & tunnel modes of IPsec

Diff

Transport mode	Tunnel mode
only payload is protected	Entire original IP packet protected
Original IP header remains	New IP header is added
Host-to-Host used	VPNs, Gateway-to-Gateway used
overhead is low	overhead is high
security level is moderate	security level is highest
It doesn't hide source/destination	It hide the source/destination

Describe various PGP services:

PGP (pretty Good privacy):

→ It is an email security tool provides confidentiality, authentication, integrity and compression

→ It uses mix of symmetric keys, private keys, digital signature and hashing

PGP (services)

1) Authentication:

It creates digital signature using private key.

process

Message → Hash (SHA/MD5) → encrypted with senders private key

↓

Attached of signature

2) Confidentiality:
It ensures privacy by encrypting the message

→ It uses receivers public key

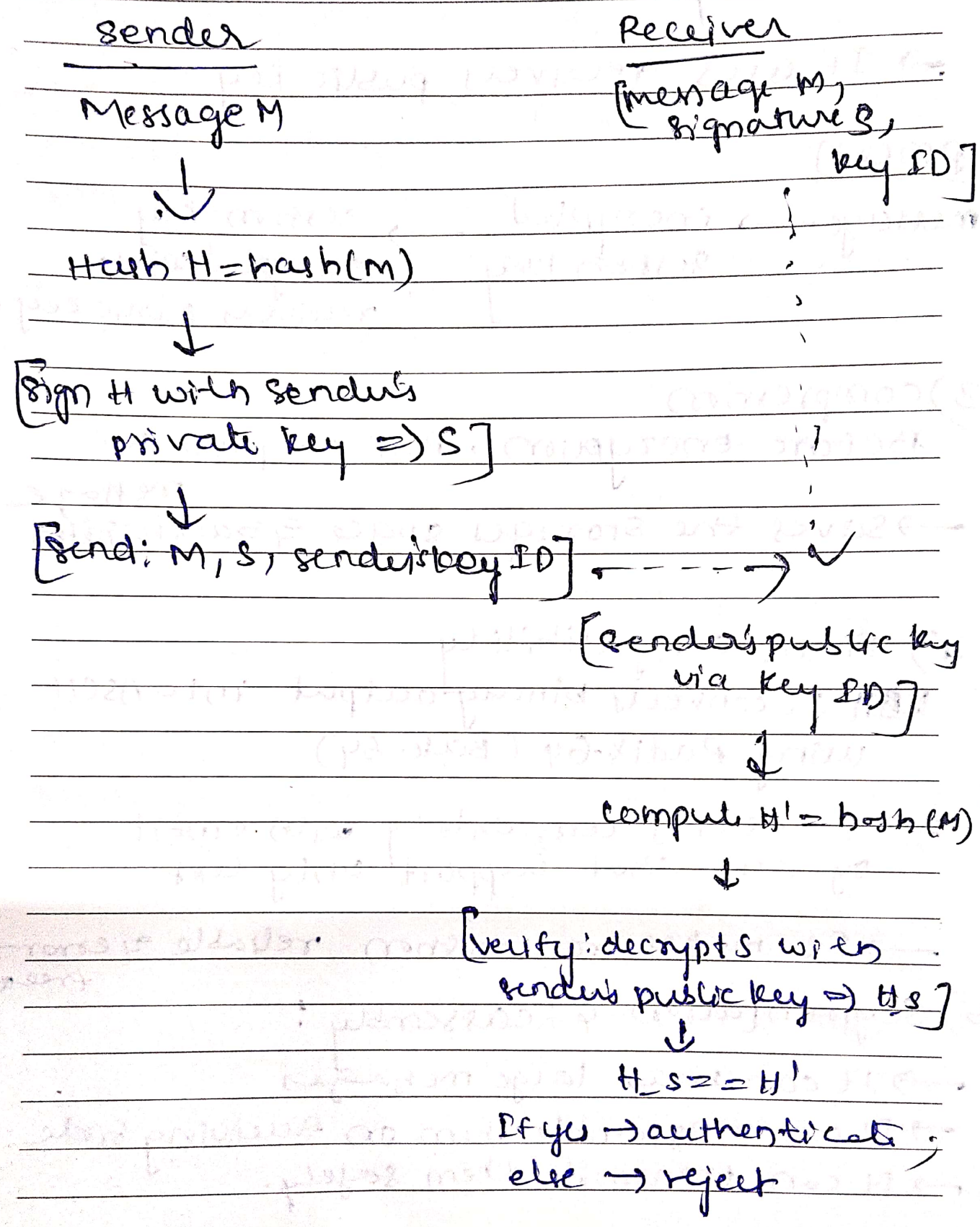
process:
message → encrypted session key → session key encrypted with receivers public key.

3) compression:
Before encryption, PGP compress the message
→ saves the storage space & bandwidth

4) Email compatibility
It converts binary output into ASCII using Radix-64 (Base-64)
→ it ensures compatibility with email systems that support only text
→ It makes transmission reliable & error free

5) Segmentation & Reassembly:
→ It can break large messages
→ It can reassemble them on receiving side
→ It can transmit them safely.

PGP cryptographic function for authentication only (diagram).



PGP provides authentication by creating a digital signature over a hash of message using sender's private key.

the receiver verifies the signature using sendys public key

confirming origin & integrity without encrypting the message

Key steps:

- Hash the message
- Sign the hash
- Transmit artifacts
- verify on receipt:

What is MIME? Difference between MIME & S/MIME:

Multi purpose Internet Mail extension

→ extension of traditional email format used in internet

→ It allows email to support text, image, audio, video, attachments and various character sets

→ MIME is a standard that enables emails to carry multimedia content, not just plain ASCII text.

Features:

- supports multiple content types
- allows attachments in an email
- uses headers to describe content type, format and encoding
- converts binary data to text using Base 64
- it enables international character sets

GOD + Desire = MAN
Man - Desire = GOD

...Bhagwan Sri Sathya Sai Baba

HPL

Differency :

Feature	MIME	S/MIME
stands for	Multipurpose Internet mail extensions	secure multipurpose Internet mail extentions
Main use	send rich content emails (text, images, audio, attachments)	Send secure emails (encrypted + digitally signed)
security	no security features	provides encryption & digital signature
encryption	not supported	supported (keeps email private
Authentication	not supported	supported (verifies sender identity)
Best for	everyday emails with multimedia	sensitive emails needing privacy & authenticity
Examples	Gmail attachments	corporate secure emails, confidential reports

fancy emails → MIME

fancy emails + security → S/MIME

Q) Functionalities of Encapsulating security payload (ESP).

ESP is a core protocol of IPsec that provides confidentiality, integrity, authentication, and anti-replay protection for IP packets

1) Confidentiality
→ ESP encrypts the payload (data) of the IP packet
→ it prevents unauthorized users from reading data
→ Uses symmetric encryption algorithms like AES, 3DES.

2) Data integrity:
ESP can ensure that data has not been modified during transmission
→ uses algorithms: HMAC, SHA

3) Authentication:
ESP can authenticate the source of packet
→ confirms the sender is genuine

4) Anti-replay protection:
ESP includes sequence of number field.
→ it protects against replay attacks

5) Limited traffic flow confidentiality:
ESP hides:
- payload
- In tunnel mode, it hides original IP header

6) Support tunnel & transport modes:
ESP works in
- Transport mode - encrypts only payload
- Tunnel mode - encrypts the entire IP packet (header + payload)

Applications of IPsec?

IPsec (Internet protocol security)

→ It is widely used to secure communication over IP networks by providing confidentiality, integrity, authentication and secure tunneling

① VPN's
- used for remote access VPNs and site-to-site

→ create secure VPN tunnels over internet

② Secure Remote Access:
→ protects sensitive data (credentials, files) from attackers on public networks

③ Secure Gateway-to-Gateway communication
→ connects two n/w securely using routers or firewalls
→ used in multi-branch companies, banks, government networks.

HPL

④ Protecting Application traffic (end-to-end security)

→ provides security like in
- e-mail
- VoIP
- File transfer
- database access

⑤ Secure Routing:

→ IPsec protects routing updates exchanged between routers
→ prevents attacks like spoofing and route manipulation

⑥ Intranet and extranet security:

→ protecting sensitive department communication
→ securing partner access (extranet)

⑦ Mobile & wireless network security:

→ used in secure communications in mobile & 5G networks
→ protects data over unsafe wireless n/w

⑧ Protecting IPv6 traffic:

→ IPsec is mandatory part of IPv6
→ Ensures secure end-to-end data protection

Draw Authentication Header (AH) & explain fields:

AH is an IPsec protocol that provides authentication, integrity and anti-replay protection but no encryption

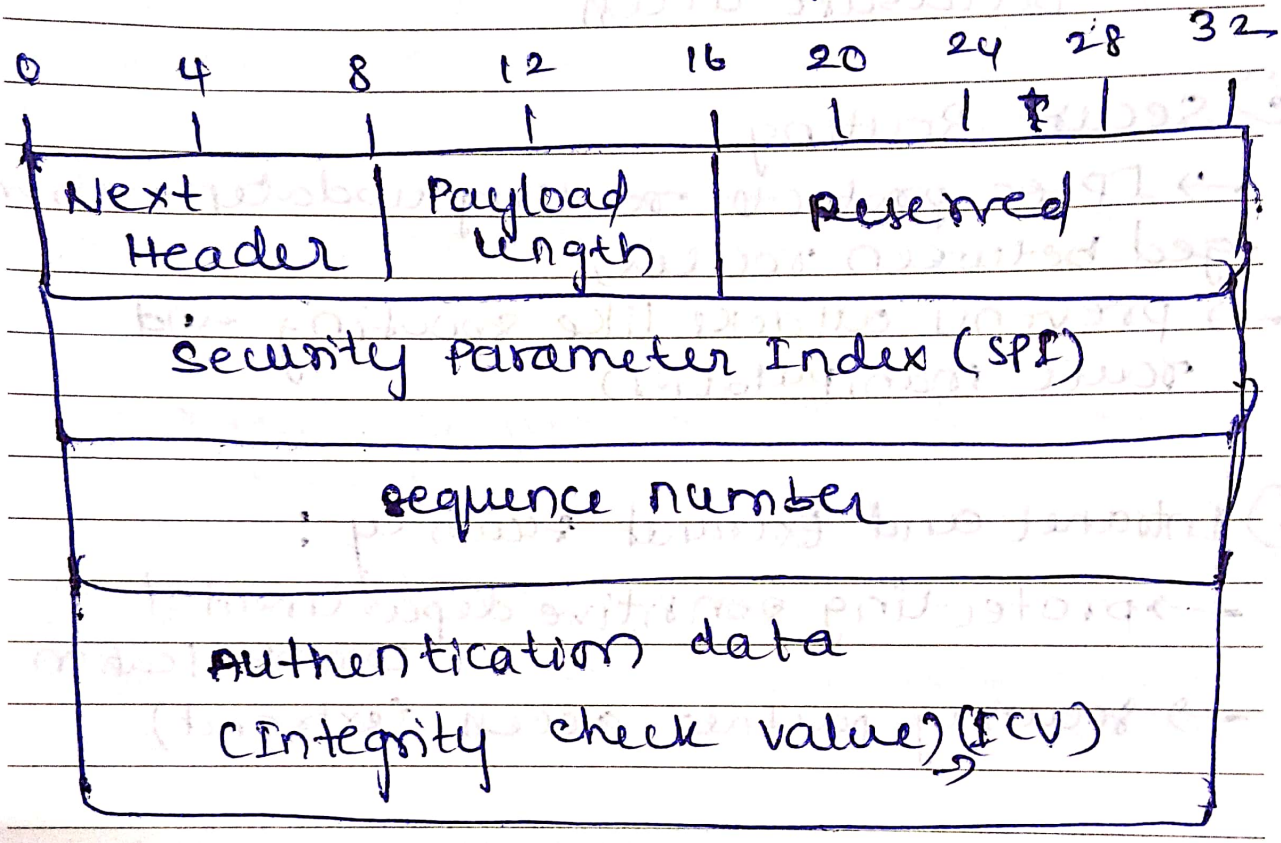


Fig. (AH) Authentication Header

Fields:

1. Next header (8 bits)
→ Identifies which type of header (protocol) that comes after AH
Eg: TCP = 6, UDP = 17, ESP = 50

HPL

② payload length (8 bits)
→ Indicates the size of AH

③ Reserved:
→ reserved for future use
→ must be set to zero

④ security Parameter Index (SPI): (32 bits)
→ Identifies the security Association (SA) for this packet
→ SA tells the receiver what algorithms/keys to use for checking authencity

⑤ sequence number (32 bits):
→ monotonically increasing no'r for each packet
→ protects against replay attacks.

⑥ ~~Authentication~~ data
→ contains integrity check value.
→ ICV is generated using hashing
→ ensures integrity & data origin authentication
→ covers most fields of IP header + data

What is radix-64? Explain PGP & S/MIME Conversion:

Radix-64:

→ It is base-64 encoding scheme used in PGP to convert binary data into ASCII text

→ since email systems originally support only text, PGP converts encrypted or signed binary data into printable characters

Why Radix-64 is needed?

→ ensure compatability with text only email systems
→ makes binary data safe for transmission
→ reduces chances of corruption
→ easy to decode back to original binary

Radix-64 output:

uses characters:
A-Z, a-z, 0-9, +, /.

Plus "=" for padding.

PGP conversion:

1. Digital signature
2. compression
3. encryption
4. Radix-64 conversion
3. Transmission

PGP conversion flow diagram:-

Message
↓
(signature) → compression → encryption → radix 64 → email

S/MIME conversion:

1. MIME formatting
2. Digital signature
3. encryption
4. Base64 Encoding (radix-64)
5. MIME packaging

S/mime conversion flow diagram

message → MIME format → (sign) → (encrypt) → Base64 → email

Q) Services provided by IPsec ?-

1. Confidentiality
2. Authentication
3. Data Integrity
4. Anti-replay protection
5. Access control
6. key management
7. Traffic flow confidentiality

Q) parameters that identify & characterize a security Association (SA)

→ A SA (security association) is a one-way logical connection that defines how IPsec protects data b/w two devices

→ Each SA is uniquely identified & described by several parameters

Parameter that Identify a SA :-

1. SPI (security parameter Index):
   → 32-bit identifier in AH/ESP header
2. Destination IP Address.
   → IP address of device (receiver) that SA is associated with
3. security protocol identifier:
   → specifies whether the SA is for AH or ESP

These three are called SA Triplet

Parameter that characterize a SA:

1. Sequence number counter
2. Sequence counter overflow flag
3. Authentication key
4. Encryption key
5. Encryption algorithm
6. Authentication Algorithm
7. Lifetime of SA
8. Mode of operation
9. Path MTU
10. Protocol parameters / Flags

Q) Limitations of SMTP & RFC-822 & how MIME overcomes them:

(used for text based email)

Limitations of SMTP & RFC-822:

1. Supports only 7-bit ASCII text:
   - → cannot send binary data, images, audio, video or documents
   - → non-english characters are not supported
2. Size restrictions
   - → cannot send large files of attachments
   - → message sizes are limited
3. No standard for Attachments:
   - → RFC-822 had no mechanism to include multiple attachments.

④ cannot Identify content type?
→ Email cannot indicate whether content is text, image, audio, application etc because it supports only plain text.

⑤ Limited character set?
→ cannot send international languages texts
→ ASCII only.

⑥ problems with Binary Transmitting
→ SMTP corrupts binary content because it is designed for text only

MIME Overcome the Limitations?

① Supports multiple content types
→ MIME introduce content-type header

② Base 64 :-
→ converts binary data to text safe format
→ solves 7-bit ASCII limitation

③ Allow Attachments:
→ MIME supports multipart messages.
→ you can attach multiple files within one email

HPL

(4) Supports different character sets
→ allow sends text in any language

(5) Handles large message.

(6) Identifies content using headers
MIME adds new headers.
→ content type
→ Content-transfer Encoding
→ content disposition

Q) Need for combining security Association (SA) & Basic SA combinations

Ans:
Need for combining security Associations:-
→ In IPsec, a SA provides security for traffic in one direction & one protocol

→ a single SA is not enough to provide all required security features.
multiple SAs must be combined.

Why combine SAs?
(1) unidirectional protection
(2) Multiple services needed
(3) Multiple tunnels
(4) Transport + tunnel.
(5) Granular policies → different types of traffic

Basic Security Association (SA) combinations:

① Transport Adjacency:
→ more than one IPsec protocol is applied at same end-to-end connection

Eg: AH+ESP both in transport mode
→ protection stays at host level

Used when: Both authentication & encryption are needed b/w same hosts without tunneling

② Tunnel Adjacency:
→ Two or more SAs applied b/w the same pair of IPsec gateways
→ All protocols operate in tunnel mode

Eg: ESP tunnel inside another ESP tunnel

Used when:

- Multi-layer VPN tunnels
- Access VPN over corporate VPN

(3) Transport - Tunnel combination:
→ one SA is in transport mode & another is in tunnel mode
Example:
→ Host-to-Host using transport
→ gateway-to-gateway using tunnel mode

used when:
→ end-to-end security + gateway-to-gateway routing protection required

---

Q) Why does ESP include a padding field?
Ans: ESP (Encapsulating security payload) includes a padding field for following reasons:

(1) Block cipher alignment:
→ encryption algorithm like AES work on fixed-size blocks
→ padding ensures the data length is a multiple of the block size, allowing proper encryption

(2) Traffic Flow confidentiality:
→ padding can be added to hide the actual length of data
- prevents attackers from guessing the type of message size

(3) ESP Trailer Alignment:
→ some systems require ESP trailer field to align 4 byte boundaries

→ It helps achieve proper alignment

(4) Support for future Algorithms:
→ padding allows flexible for future encryption or authentication schemes may need specific alignment