Unit - III (IP Security Architecture)

IP Security Architecture

- Overview , Authentication Header, Encapsulating Security Pay Load Combining Security Associations, Key Management.

IP Security (IPsec) is a **network-layer security protocol** used to protect data sent over an IP network (like the Internet).

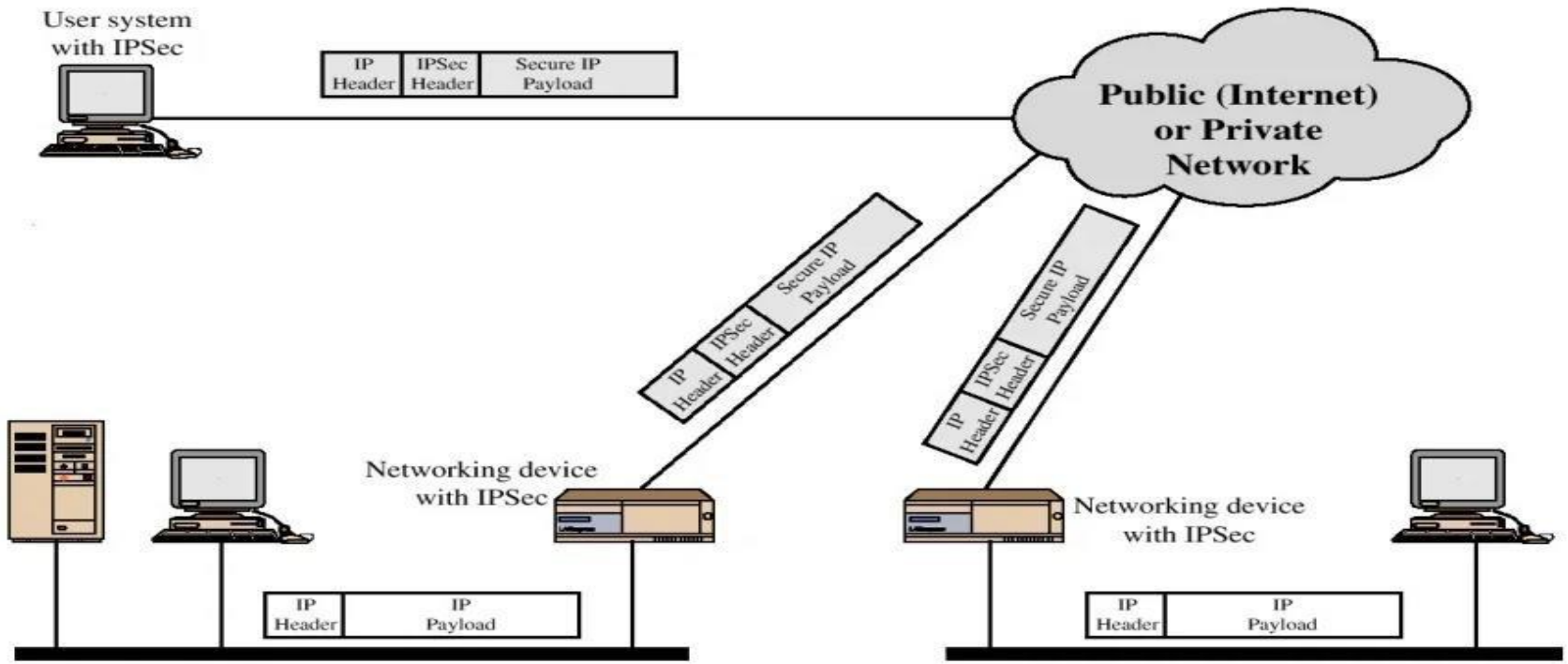
It provides **secure communication between two computers or networks**.

What is IP Security (IPSec)?
IPSec (Internet Protocol Security) is a set of protocols used to secure data communication over a network (like the Internet).
It works at the Network Layer (Layer 3) of the OSI model.

Main purpose:

Protect data from hackers
Ensure secure communication between systems

IP Security Scenario



1. **User System with IPsec**

•The sender's computer has **IPsec enabled**

•Normal IP packet is converted into:

- **IP Header**
- **IPsec Header (AH/ESP)**
- **Secure IP Payload (encrypted data)**

Data becomes **secure before leaving the system**

2. **Transmission over Public / Private Network**

•The packet travels through the **Internet (unsafe network)**

•Even if attackers capture the packet:

- Data is **encrypted**
- Data **cannot be read or modified**

3. Networking Device with IPsec (Gateway / Router)

•IPsec-enabled routers act as **security gateways**

•Commonly used in **VPNs**

•They:

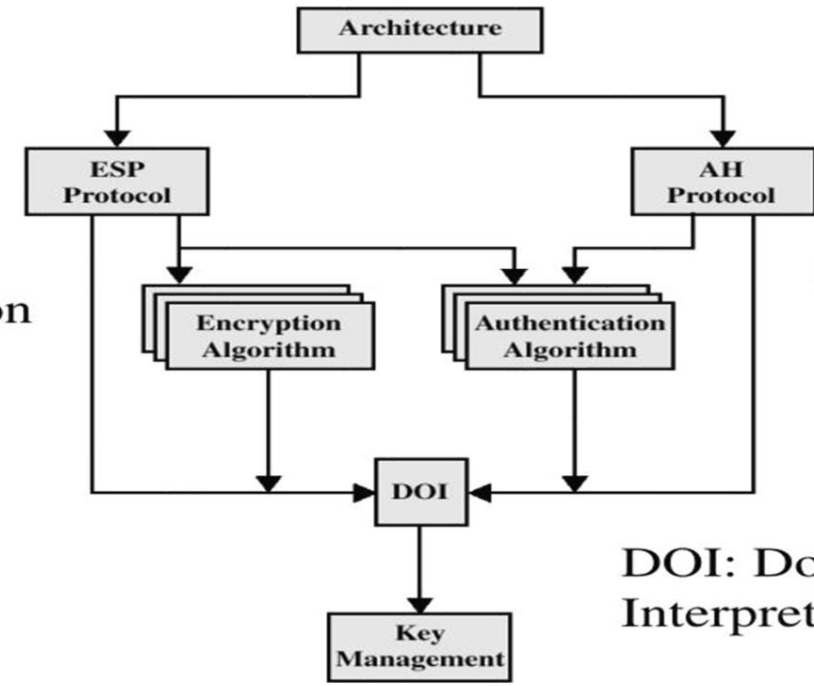
- Encrypt outgoing packets
- Decrypt incoming packets
- Authenticate sender and receiver

4. Receiving Side

•Destination device or gateway:

- **Verifies authentication**
- **Decrypts payload**
- Delivers original IP payload to the user

IPSec Document Overview



ESP:
Encapsulation
Security
Payload

AH:
Authentication
Header

DOI: Domain of Interpretation

1. IPSec Architecture

•Overall framework that defines **how security is provided at the IP layer**.

•Uses two main protocols: **ESP** and **AH**.

2. ESP (Encapsulating Security Payload)

•**Purpose:** Protects data.

•**Provides:**

- **Encryption** (confidentiality)
- Optional authentication & integrity

•Uses **Encryption Algorithms** (like AES).

•Mostly used in real networks because it keeps data **secret**.

3. AH (Authentication Header)

- **Purpose:** Verifies sender and data integrity.
- **Provides:**
  - **Authentication**
  - **Integrity**
- **No encryption** (data is visible).
- Uses **Authentication Algorithms** (like HMAC).

4. Encryption Algorithm

- Used by **ESP**.
- Encrypts the actual data so attackers cannot read it.

5. Authentication Algorithm

•Used by **ESP (optional)** and **AH**.

•Ensures:

- Data is not changed
- Sender is genuine

6. DOI (Domain of Interpretation)

•Defines **rules and formats** for:

- Algorithms
- Keys
- Security parameters

•Helps both ends understand each other correctly.

7. Key Management

•Manages **creation, exchange, and deletion of keys**.

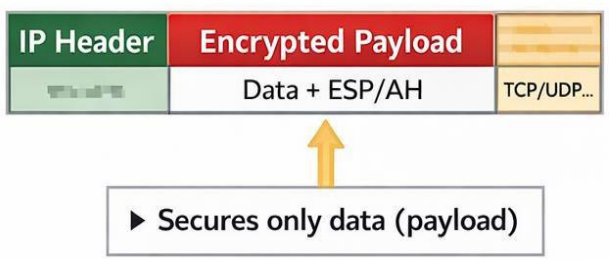
•Commonly done using **IKE (Internet Key Exchange)**.

IP Security (IPSec) Modes

1. Transport Mode:

Transport Mode

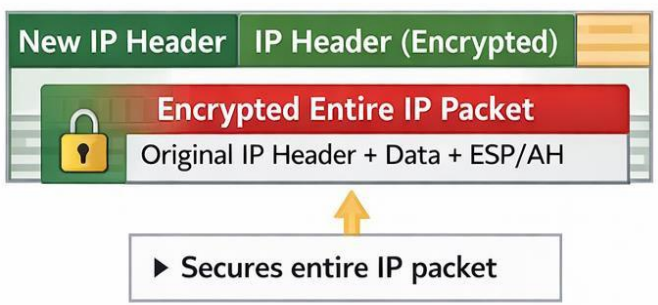
- Encrypts/authenticates only the data (payload)
- Used for host-to-host communication



2. Tunnel Mode:

Tunnel Mode

- Encrypts/authenticates entire IP packet
- Used for VPNs (network-to-network / host-to-network)



IP Security (IPSec) Modes –
IPSec has **two modes**:
1. Transport Mode
•Encrypts/authenticates **only the data (payload)**
•IP header remains visible
•Used for **host-to-host** communication

2. Tunnel Mode
•Encrypts/authenticates **entire IP packet**
•New IP header is added
•Used for **VPNs (network-to-network / host-to-network)**
In short:
•**Transport mode → partial protection**
•**Tunnel mode → full protection**

IP Security (IPSec) Protocols

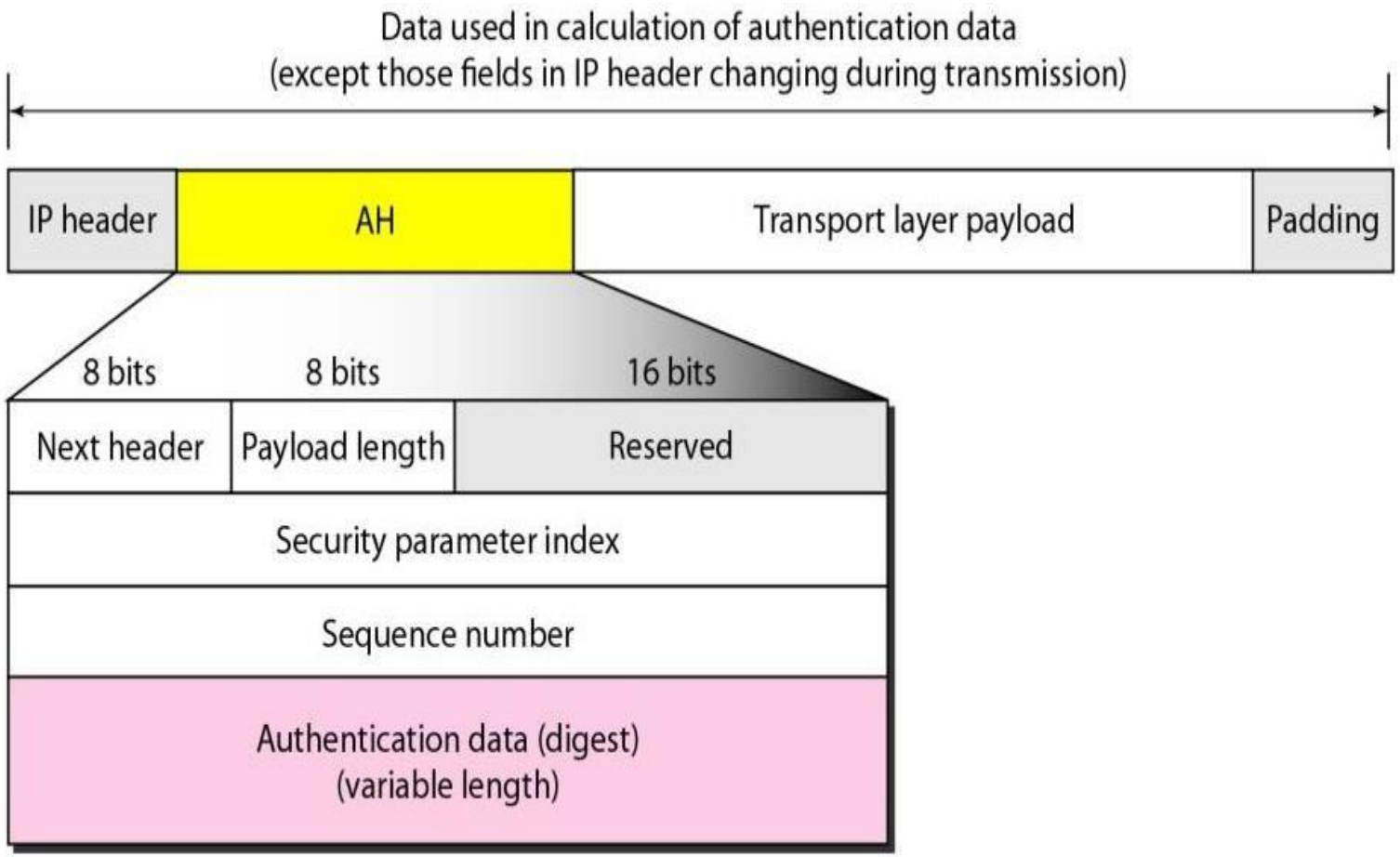
1. AH (Authentication Header)

- ✔ Provides **authentication** and data **integrity**
- ✘ **No** encryption
- ✔ Ensures data is not altered

2. ESP (Encapsulating Security Payload)

- 🔒 Provides **encryption** (confidentiality)
- ✔ Also provides **authentication** & integrity (optional)
- ✔ Most commonly used protocol

AH → Authentication | **ESP → Encryption + Security** | **IKE → Key exchange**


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Transport layer payload
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

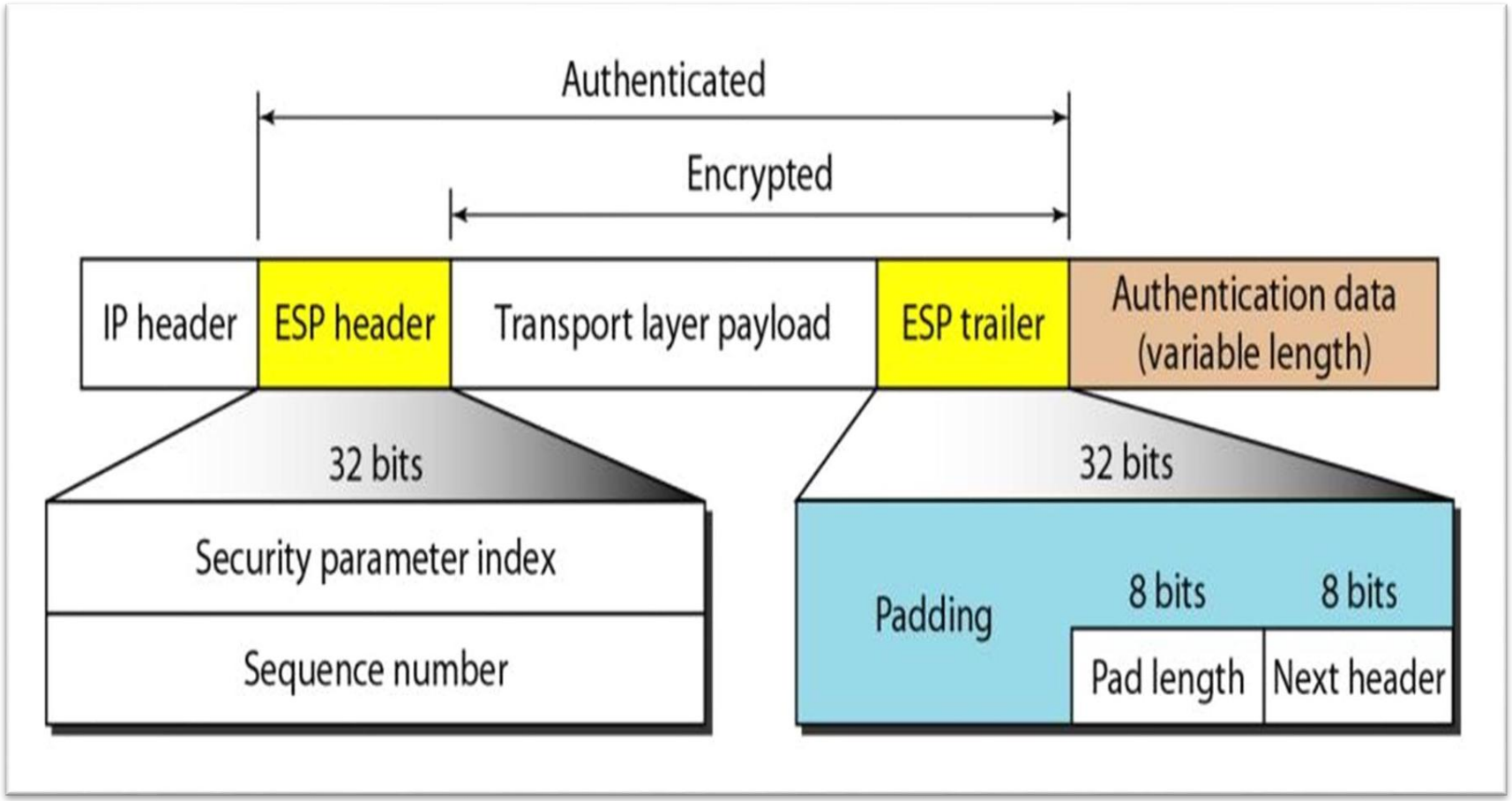
AH (Authentication Header)

AH Position

- AH is placed **after the IP header** and **before the transport layer payload**.
- It protects **IP header (except changing fields)** and **data**.

Fields in AH Header

1. **Next Header (8 bits)**
   1. Indicates the next protocol (TCP, UDP, ICMP, etc.).
2. **Payload Length (8 bits)**
   1. Length of the AH header.
3. **Reserved (16 bits)**
   1. For future use (set to zero).
4. **Security Parameter Index – SPI**
   1. Identifies the **Security Association (SA)**.
5. **Sequence Number**
   1. Prevents **replay attacks**.
6. **Authentication Data (Digest)**
   1. Message authentication code (MAC).
   2. Ensures **data integrity and sender authentication**.
   3. Variable length.


Authenticated
Encrypted
IP header
ESP header
Transport layer payload
ESP trailer
Authentication data
(variable length)
32 bits
Security parameter index
Sequence number
32 bits
Padding
8 bits
8 bits
Pad length
Next header

ESP (Encapsulating Security Payload)
ESP Position
•ESP is placed **after the IP header**.
•It protects the **transport layer payload**.
Parts of ESP

1. ESP Header
•**Security Parameter Index (SPI – 32 bits)**
→ Identifies the Security Association (SA).
•**Sequence Number (32 bits)**
→ Protects against replay attacks.

2. Encrypted Portion
•**Transport Layer Payload** (TCP/UDP data)
•**ESP Trailer**, which includes:
- **Padding** – for block size alignment
- **Pad Length (8 bits)** – length of padding
- **Next Header (8 bits)** – type of data(TCP/UDP)

This whole part is **encrypted**.

3. Authentication Data
•Variable length
•Provides **integrity & authentication**
•Optional (depends on configuration)

Combining Security Associations (SA) in IPSec

In IPSec, **Security Associations (SAs)** can be **combined** to provide multiple security services together.

Why combine SAs?

•One SA gives **limited security**

•Combining SAs gives **stronger protection** (authentication + encryption)

Types of SA Combinations

- **1. Transport Adjacency**
  - Multiple SAs applied**one after another**
  - Example:
    AH (authentication) + ESP (encryption)
  - Used when both services are needed separately

2. IteratedTunneling

- One SA is applied**inside another SA**
- Example:
  ESP tunnel inside AH tunnel
- Common in**VPNs**

Key Management in IPSec

Key Management is the process of creating, exchanging, and managing cryptographic keys used by IPSec.

Why Key Management is needed?

•Encryption & authentication require secret keys

•Keys must be exchanged securely

IKE (Internet Key Exchange)

•IPSec uses IKE for key management

•It:

- Authenticates both parties
- Exchanges keys securely
- Creates Security Associations (SAs)

The **IPSec architecture document mandates support for two types of key management**:

- **1. Manual Key Management**
  - Keys are **manually configured** by the administrator.
  - No automatic key exchange
  - No key refresh
  - Simple but **not secure**
  - Used only for **testing or small networks**

- **2. Automatic Key Management (IKE)**
  - Uses **IKE (Internet Key Exchange)** protocol.
  - Automatic key generation
  - Secure key exchange
  - Periodic key refresh
  - Scalable and secure
  - Used in **real-world IPSec implementations**

ISAKMP/Oakley in IPSec

•The **default automated key management protocol for IPSec** is called **ISAKMP/Oakley**.

ISAKMP (Internet Security Association and Key Management Protocol)

•Defines the **framework** for:

- Security Association (SA) rule creation
- Authentication
- Key management

•Does **not** define how keys are generated.

Oakley

•Defines the **key exchange mechanism**

•Uses **Diffie–Hellman** to generate shared secret keys securely

Together (ISAKMP + Oakley)

•ISAKMP provides the **structure**

•Oakley provides the **key exchange**

•Combined to form **IKE (Internet Key Exchange)**

Features of OAKLEY

OAKLEY is a **key exchange and management protocol** used with ISAKMP in IPsec.

1. **Secure Key Exchange**

   Uses **Diffie–Hellman** to generate shared secret keys securely.

2. **Perfect Forward Secrecy (PFS)**

   Compromise of one key does not affect past or future keys.

3. Authentication Support

Supports authentication using:

1. Pre-shared keys
2. Digital signatures
3. Public-key encryption (Public key , private key)

4. Identity Protection

Protects the identities of communicating parties during exchange.

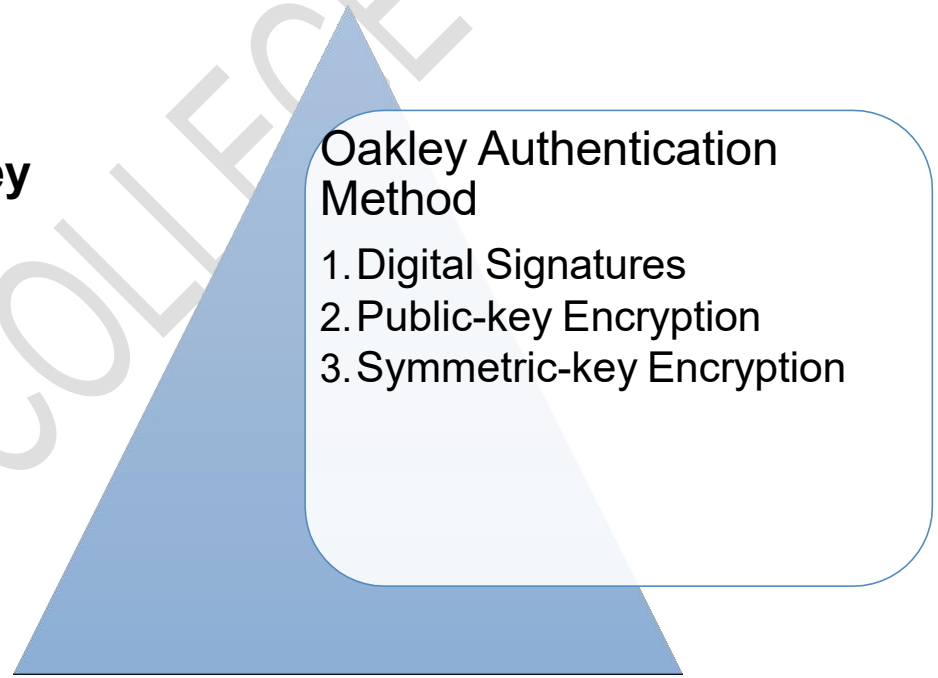
5. Algorithm Independence

Independent of encryption and hash algorithms. Ex pin , pattern , face lock

Oakley Authentication Methods

1. Digital Signature

- Uses **public–private key pair**
- Sender signs authentication data with **private key**
- Receiver verifies using **sender's public key**
- Strong authentication
- Prevents impersonation



2.Public Key Encryption

•Authentication data is encrypted using **receiver's public key**

•Receiver decrypts it using **private key**

• Secure identity verification

• Slower than symmetric methods

3. Symmetric Key Encryption (Pre-Shared Key)

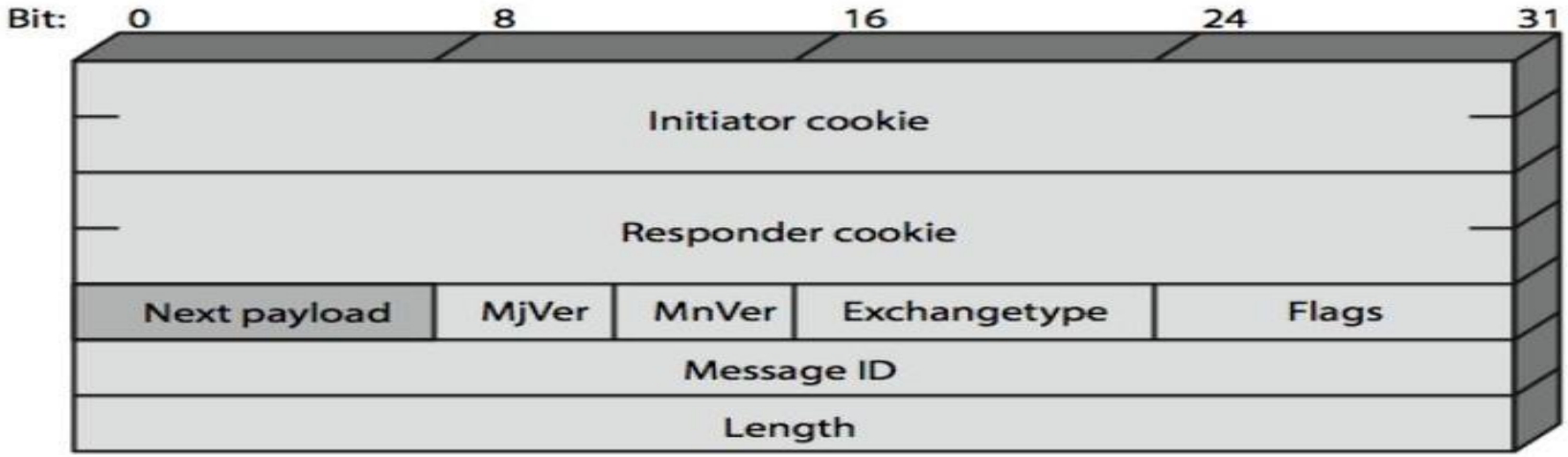
•Both parties share a **secret key in advance**

•Authentication data encrypted using the **same key**

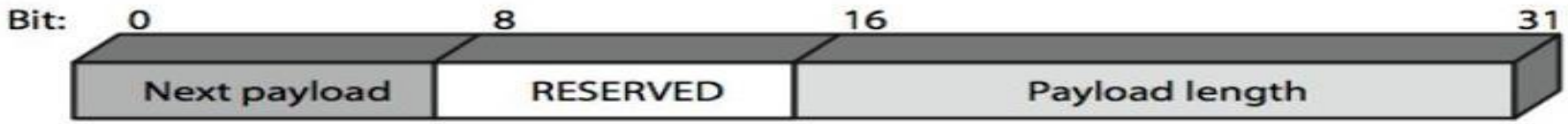
• Fast and simple

• Less secure, key distribution problem

ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

ISAKMP Payload Types

1. Proposal Payload
•Contains a set of security proposals.
•Specifies protocols, algorithms, and parameters for the Security Association (SA).

2. Transform Payload
•Defines the specific cryptographic algorithms within a proposal.
•Includes encryption, hash, authentication methods, etc.

i. Key Exchange Payload
Used to exchange keying material.
Supports algorithms like Diffie–Hellman for secure key generation.

ii. Identification Payload
Identifies the initiator or responder.
Contains information such as IP address or hostname.

3. Certificate Payload

Carries **digital certificates**.

Used for authentication of communicating parties.

3.1 Hash Payload

Provides **data integrity and authentication**.

Verifies that the message has not been altered.

3.2 Signature Payload

Contains a **digital signature**.

Used for authentication using public-key cryptography.

3.3 Nonce Payload

Contains a **random number**.

Prevents replay attacks and ensures freshness of communication.

3.4 Notification Payload

Used to send **error messages or status information**.

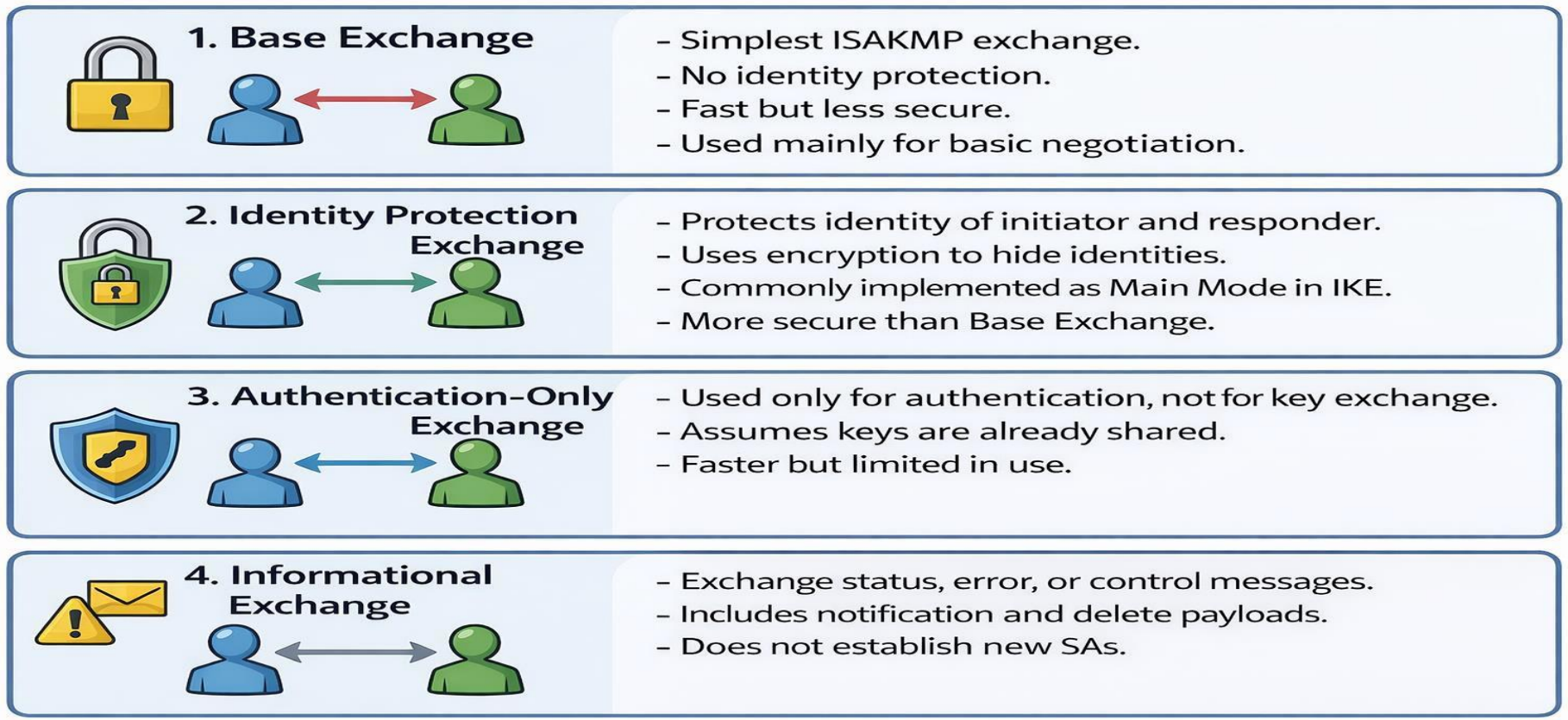
Indicates problems or success of exchanges.

4. Delete Payload

Used to **delete an existing Security Association (SA)**.

Terminates IPsec or ISAKMP sessions.

ISAKMP Exchanges



ISAKMP Exchanges

ISAKMP defines different **exchange types** to establish and manage Security Associations.

1. Base Exchange

Simplest ISAKMP exchange.
No identity protection.
Fast but **less secure**.
Used mainly for basic negotiation.

2. Identity Protection Exchange

Protects the **identity of initiator and responder**.
Uses encryption to hide identities.
Commonly implemented as **Main Mode** in IKE.
More secure than Base Exchange.

3. Authentication-Only Exchange
Used **only for authentication**, not for key exchange.
Assumes keys are already shared.
Faster but limited in use.

4. Informational Exchange
Used to exchange **status, error, or control messages**.
Includes **notification and delete payloads**.
Does not establish new Security Associations.

Very Short Questions

1. What is the main purpose of IP Security (IPSec)?
2. Define Authentication Header (AH).
3. Define Encapsulating Security Payload (ESP).
4. What is a Security Association (SA)?
5. Name two types of IPSec modes.
6. What does AH provide: confidentiality or integrity?
7. What is the role of key management in IPSec?
8. Which protocol provides encryption in IPSec?
9. What is the difference between transport and tunnel mode?
10. What does IPSec protect: data at rest or data in transit?

Short Questions

1. Explain the difference between AH and ESP.
2. What is the structure of a Security Association in IPSec?
3. How does combining multiple Security Associations enhance security?
4. Describe the purpose of key management in IPSec.
5. List the components of IPSec architecture.

Long Questions

1. Explain the working of the Authentication Header (AH) in IPSec, including how it ensures integrity and authentication of packets.

2. Discuss Encapsulating Security Payload (ESP) in detail and explain how it provides confidentiality, integrity, and authentication.

3. Explain Security Associations (SA) in IPSec. How are they established, and what is their role in securing communication?

4. Describe the key management mechanisms used in IPSec, including manual keying and automated protocols like IKE.

5. Explain the overall IPSec architecture. Discuss how AH, ESP, Security Associations, and key management work together to provide secure communication.