Security Architecture for the Internet Protocol: IPSEC

Víctor A. Villagrá

Associate Professor

Telematics Department (DIT)

Technical University of Madrid (UPM)

IPSEC

- ❑ Objective: to provide security mechanisms to IP (IPv4 or IPv6)

- ❑ Security Services
  - ▪ Integrity in a Connectionless Environment
  - ▪ Access Control
  - ▪ Authentication
  - ▪ Anti-replay Mechanisms
  - ▪ Data Confidentiality
  - ▪ Limited traffic flow confidentiality

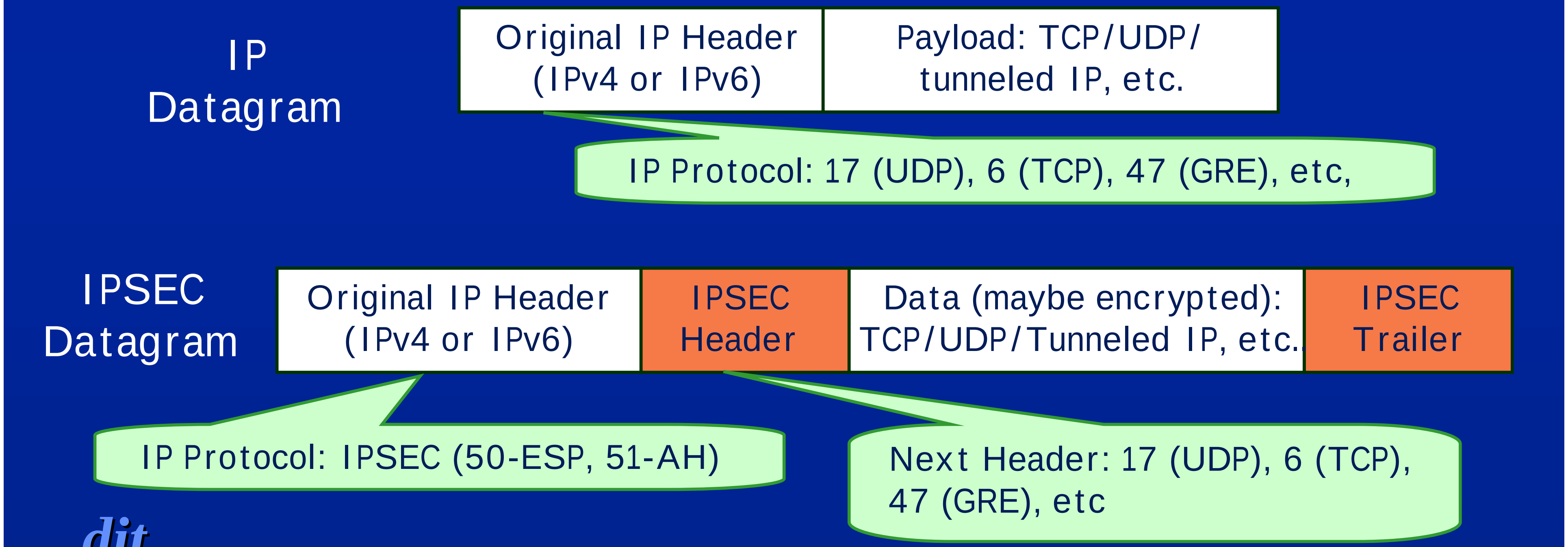
IPSEC Scope

- ❑ IPSEC has three main functionalities:
  - Authentication Only
    - ✓Known as Authentication Header (AH)
  - Encryption + Authentication
    - ✓Known as Encapsulating Security Payload (ESP)
  - A key management functions
    - ✓IKE (ISAKMP / Oakley)

- ❑ IPSEC does not define the security algorithms to use:
  - Framework which allows the participating entities to choose among multiple algorithms.

IPSEC Scope

- ¿How is IPSEC transmitted?
  - A new header in the IP datagram between the original header and the payload
  - In ESP, data are encrypted and a new datagram trailer is added



IP Datagram

Original IP Header (IPv4 or IPv6)

Payload: TCP/UDP/ tunneled IP, etc.

IP Protocol: 17 (UDP), 6 (TCP), 47 (GRE), etc,

IPSEC Datagram

Original IP Header (IPv4 or IPv6)

IPSEC Header

Data (maybe encrypted): TCP/UDP/Tunneled IP, etc..

IPSEC Trailer

IP Protocol: IPSEC (50-ESP, 51-AH)

Next Header: 17 (UDP), 6 (TCP), 47 (GRE), etc

IPSEC Security Association (SA)

- ❑ Interoperability environment used in AH and ESP
- ❑ One-to-one relationship between sender and receiver which define the set of security parameters used
- ❑ A SA establishment is needed before any communication: IKE
- ❑ SA contents:
  - ▪ Security Parameter Index (SPI)
  - ▪ IP Destination Address
  - ▪ Security Protocol Identifier

Security Association (SA)

❑ Security Parameter Index (SPI)

- Bitstring assigned to the SA with local meaning.
  - ✓Pointer to a SA data base (SPD: Security Policy Database).
- It is transmitted in the AH and ESP headers for selecting the SA which will process the message

❑ IP Destination Address

- Only unicast addresses allowed.

❑ Security Protocol Identifier (SPI):

- AH (authentication only)
- ESP (encryption and optionally authentication)

¿ What is defined by a SA?

- ❑ *Sequence Number Information:*
  - A sequence number, overflow action and anti-replay window for assuring integrity of datagrams.
  - 32 bits value used to generate the sequence number transmitted in the AH and ESP headers
- ❑ *Security Information:*
  - Authentication algorithms, keys, lifetimes, etc. used in AH or ESP
- ❑ *IPSEC Protocol Mode:* Transport, tunnel or wildcard
- ❑ *SA Lifetime:* Time or bytes interval of a SA.
- ❑ *Path MTU:* Maximum packet size transmitted without fragmenting them

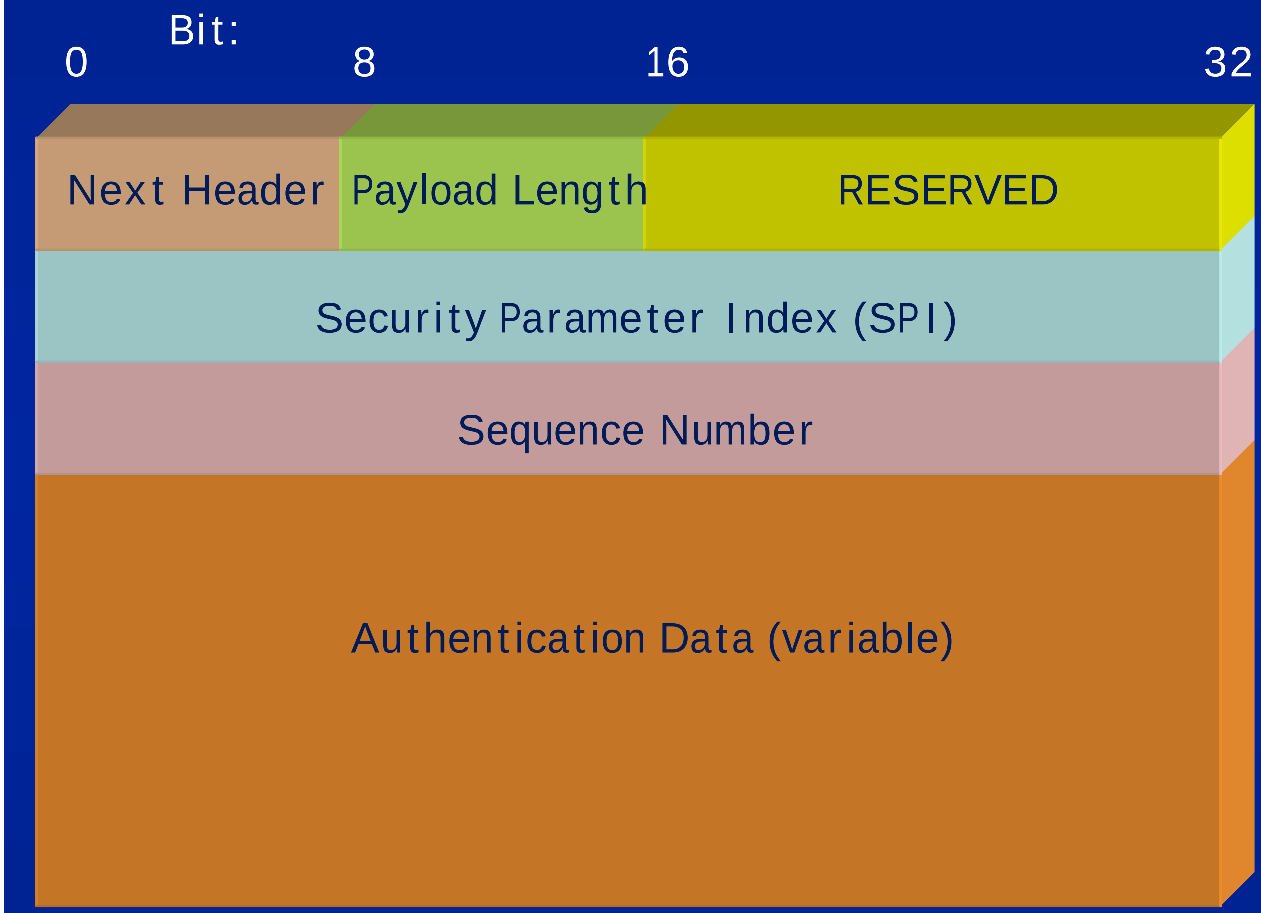
Authentication Mode: AH

- AH: Authentication Header

- It provides support for the authentication and integrity of the IP datagrams.

  - Changes in the content are detected
  - Receivers can authenticate the sender
  - It avoids the IP-Spoofing attack
  - It provides protection against the replay attack.

IPSEC Authentication Header (AH)



Bit:

0 8 16 32

Next Header | Payload Length | RESERVED

Security Parameter Index (SPI)

Sequence Number

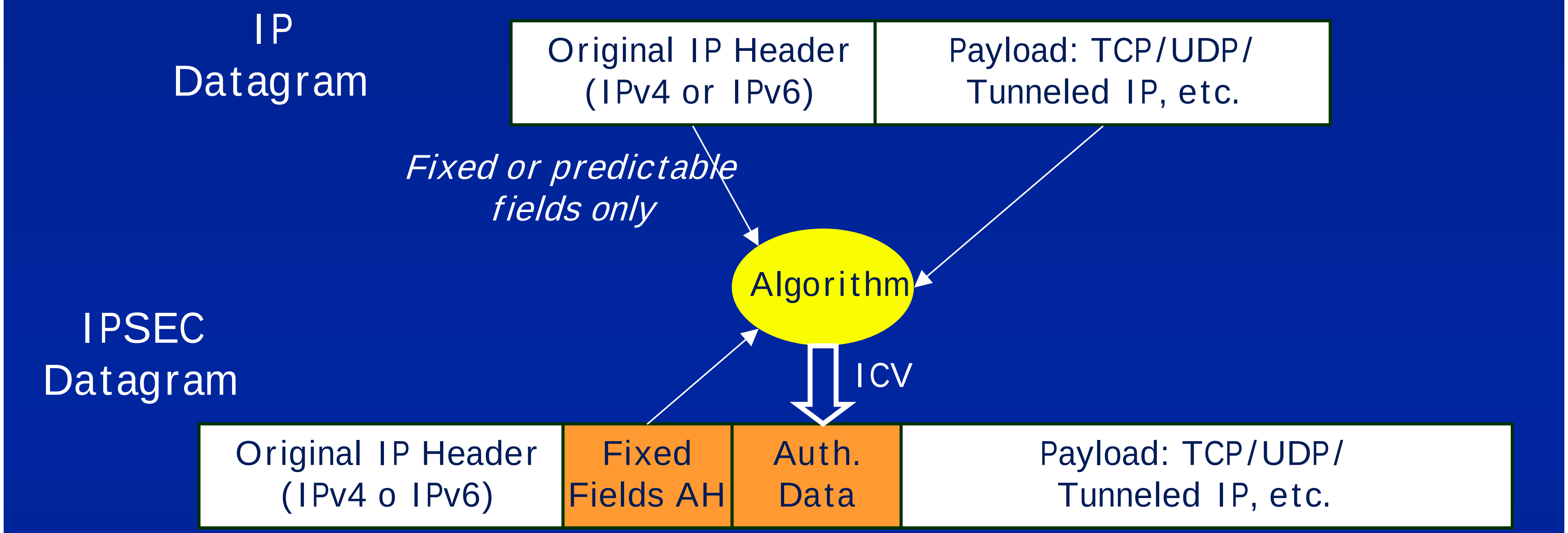
Authentication Data (variable)

- Next Header: data protocol transmitted inside IP
- Payload Length: Length of the AH header
- Security Parameter Index (SPI): identification of the SA of this datagram
- Sequence Number: counter incremented with each packer
- Authentication Data: Integrity Check Value (ICV)

Authentication Header (AH)

- ❑ Authentication is based on the use of the *Integrity Check Value*, with an algorithm specified in the SA.
- ❑ Input: message digest and secret key
- ❑ Output: ICV transmitted in the Authentication Data field of the AH
- ❑ The algorithm is applied to:
  - ▪ The whole datagram payload
  - ▪ Fields of the IP header which do not change in transit or are predictable.
  - ▪ The AH header, except the Authentication Data field
- ❑ Algorithms: at least MD5 and SHA-1 for interoperability

Authentication Data



Mutable fields in the IPv6 header

- ❑ Class
- ❑ Flow Label
- ❑ Hop Limit

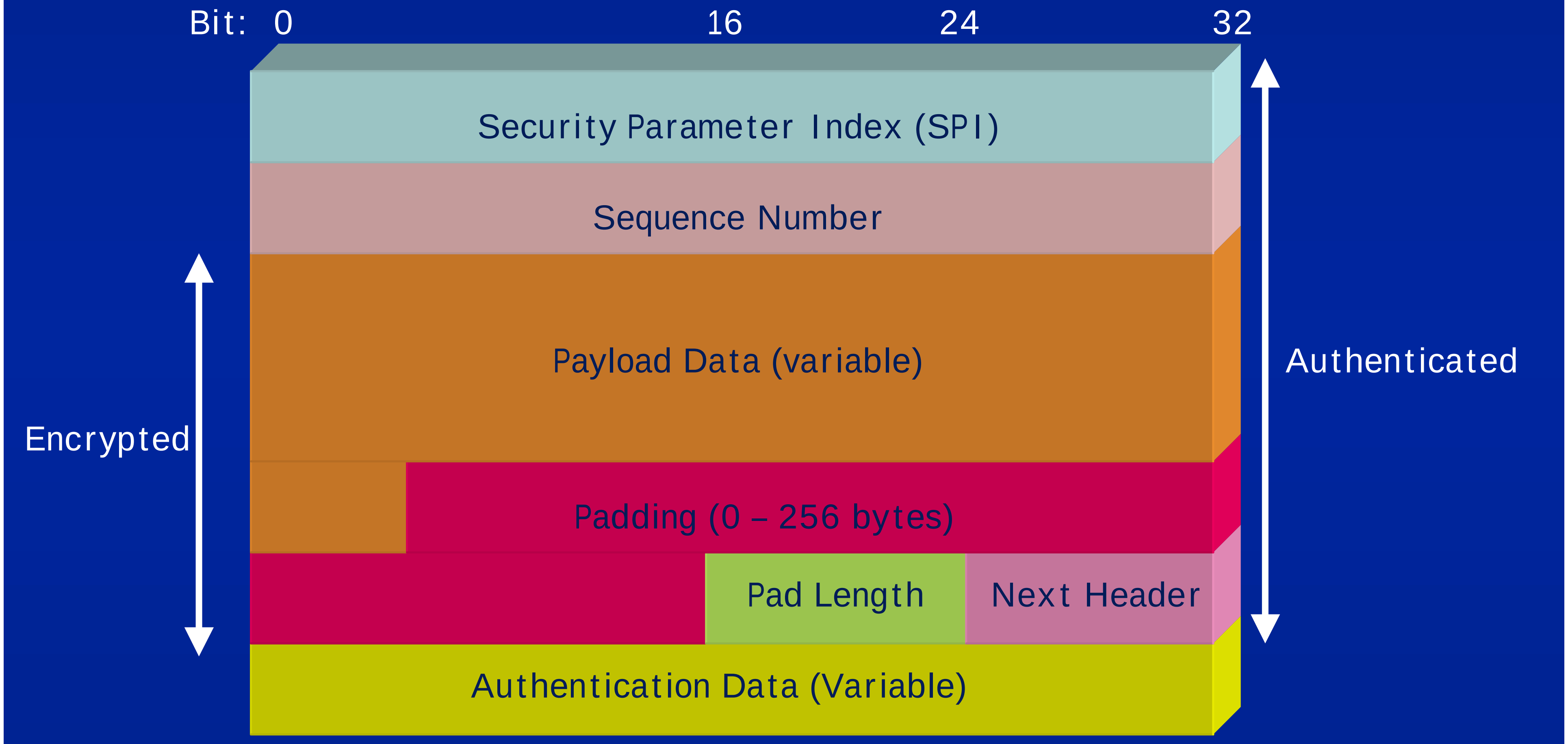
Predictable fields in the IPv6 header

- ❑ Destination Address

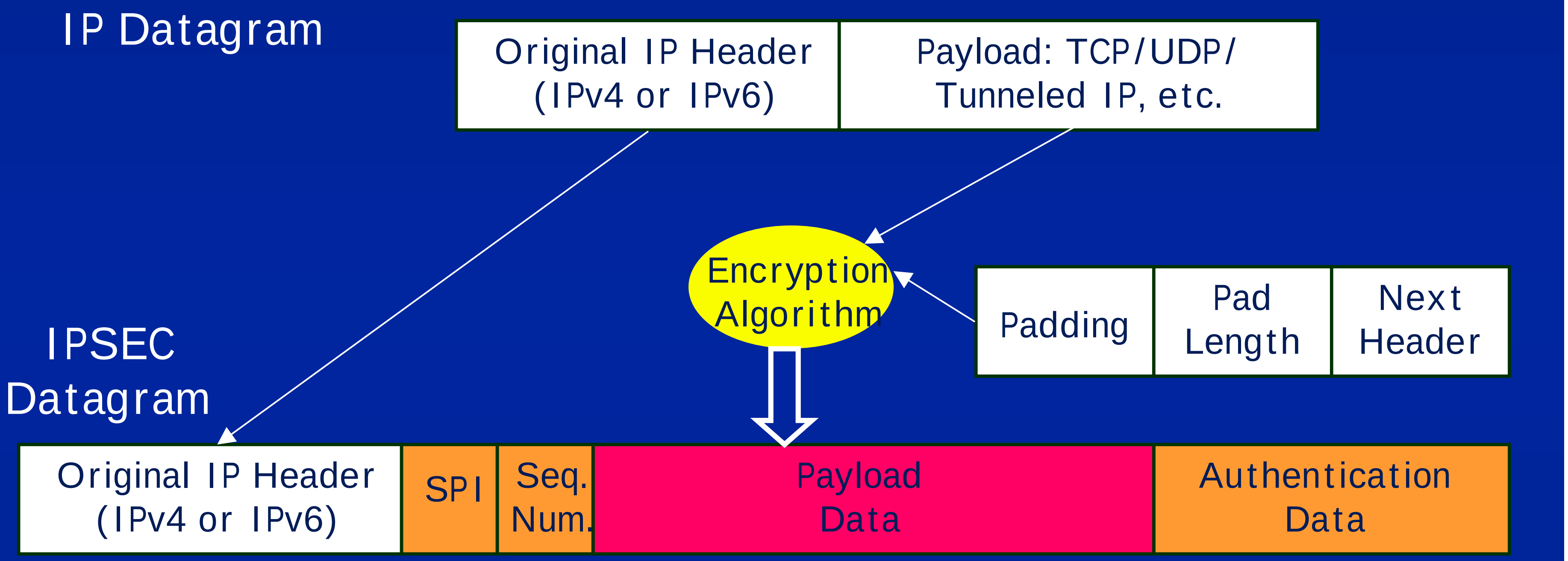
Encryption Mode: ESP

- ESP: Encapsulating Security Payload
- It provides:
  - Content confidentiality
  - Limited traffic flow confidentiality
  - Optionally, authentication services like AH
- Contents of the ESP datagram:
  - Security Parameter Index (SPI): SA of this datagram.
  - Sequence Number: counter incremented with each packet
  - Payload Data: Encrypted data of the IP Protocol
  - Padding: when needed by the encryption algorithm
  - Pad Length: Number of padding bytes
  - Authentication Data: ICV computed over all the datagram
  - Next Header: Data protocol in the payload data

Format of the ESP Datagram



ESP computation

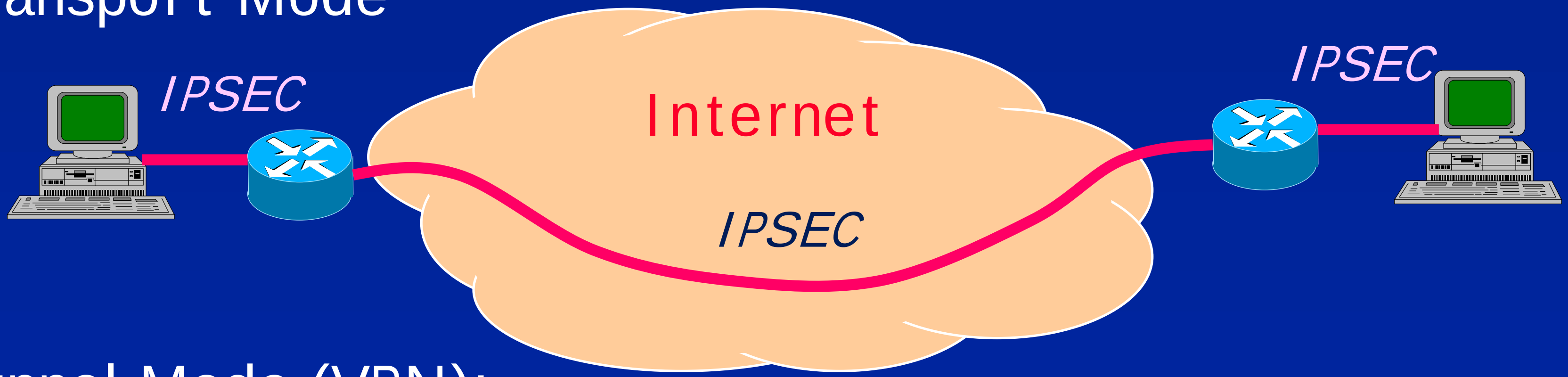


Cryptographic Algorithms

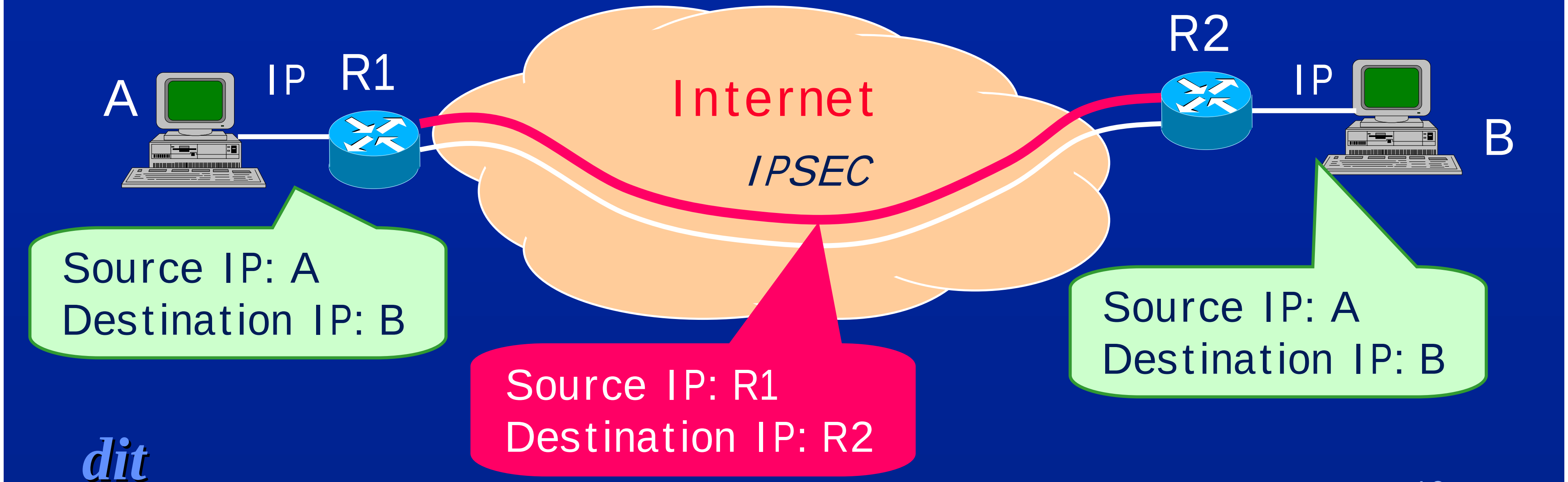
- Specified in the SA
- For encryption, it is used symmetric algorithms
- For interoperability, the following ones should be supported
  - DES with CBC mode for encryption
  - MD5 and SHA-1 for authentication
- There are many others that may be used (with an id):
  - Triple DES, RC5, IDEA, CAST, Blowfish, etc.

Transport and Tunnel Mode

Transport Mode



Tunnel Mode (VPN):

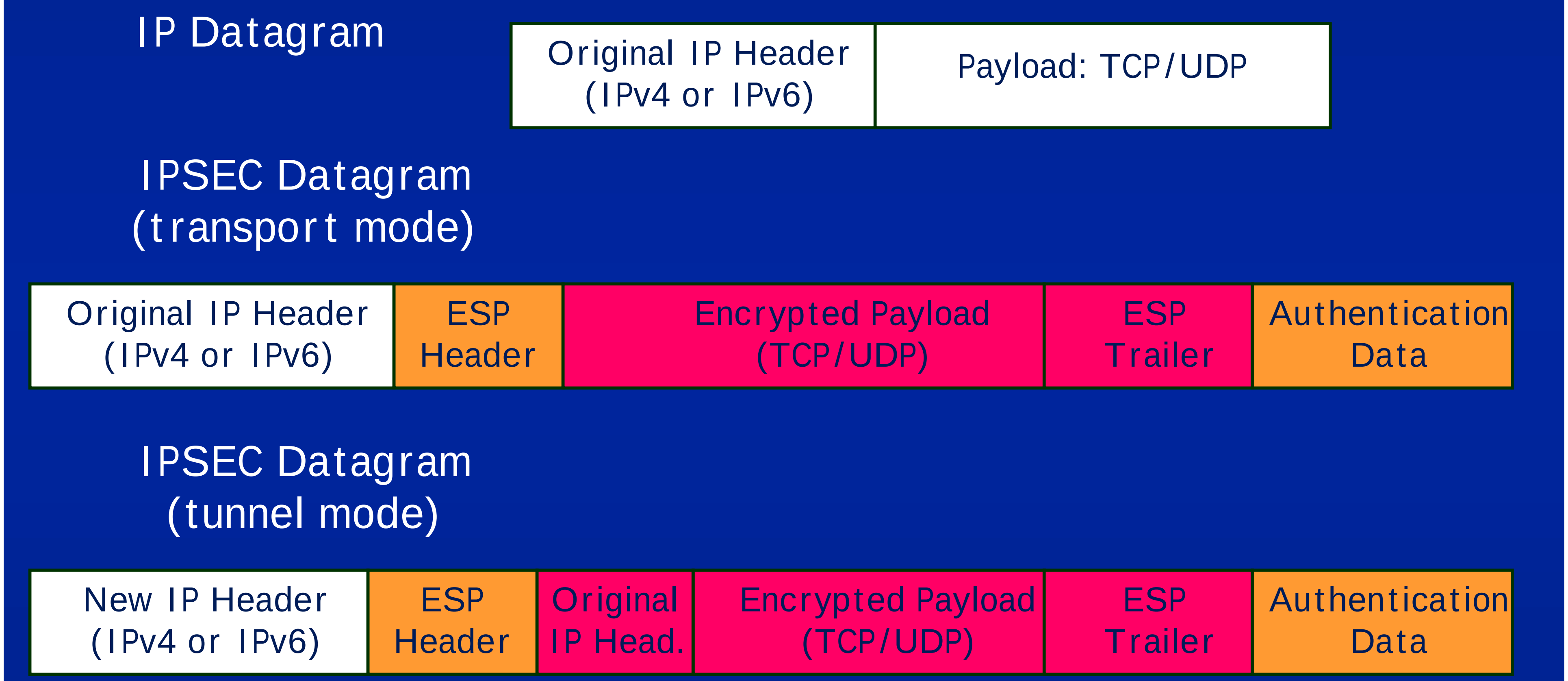


Source IP: A
Destination IP: B

Source IP: R1
Destination IP: R2

Source IP: A
Destination IP: B

Transport and Tunnel Mode



IP Datagram

Original IP Header (IPv4 or IPv6)	Payload: TCP/UDP

IPSEC Datagram (transport mode)

Original IP Header (IPv4 or IPv6)	ESP Header	Encrypted Payload (TCP/UDP)	ESP Trailer	Authentication Data

IPSEC Datagram (tunnel mode)

New IP Header (IPv4 or IPv6)	ESP Header	Original IP Head.	Encrypted Payload (TCP/UDP)	ESP Trailer	Authentication Data

Key Management

- Default Protocol for Key Management in IPSEC: IKE (Internet Key Exchange)
- Standard Method for:
  - Dynamically authenticate IPSEC peers
  - Negotiate security services
  - Generate shared keys
- Two components:
  - ISAKMP: procedures and packet formats for the establishment, negotiation, modification and deletion of a SA.
  - OAKLEY: Key exchange protocol.

OAKLEY

- ❑ Key Determination Protocol
- ❑ Main objective: generation of a session key shared by both peers.
- ❑ Method: : Diffie-Hellman algorithm (modified)
  - ▪ Previous agreement on:
    - ✓ A large primus number: q
    - ✓ A primitive root of q: a (a mod q, a^2 mod q, .. a^{q-1} mod q are different)
  - ▪ A selects X_A (secret) and transmits to B: $Y_A=a^{X_A}$
  - ▪ B selects X_B (secret) and transmits to A: $Y_B=a^{X_B}$
  - ▪ Both compute $K=(Y_B)^{X_A}$ mod $q=(Y_A)^{X_B}$ mod q
  - ▪ It is modified for authenticating the peers and avoiding the "man-in-the-middle" attack.

OAKLEY

- ❑ Goal: having a shared key between two authenticated identities
- ❑ Basic protocol components:
  - Cookies exchange
  - Diffie-Hellman half-keys exchange
  - Authentication.
- ❑ It is possible to make it with a different number of transaction (ISAKMP modes)
- ❑ Authentication:
  - Pre-shared key
  - DNS public keys (DNSSEC)
  - RSA public keys without certificates (PGP)
  - RSA public keys with certificates
  - DSS public keys with certificates

ISAKMP

- Procedures and formats for the establishment, negotiation, modification and deletion of a SA.
- Exchanges in ISAKMP:
  - Base: key exchange and authentication together
  - Identity Protection: first key exchange and then authentication
  - Authentication Only: without key exchange
  - Aggressive: key exchange and authentication minimizing the number of transactions
  - Informational: one-way for SA management.