Security in IP (IPv4 and IPv6): IPSEC

Dr. Víctor A. Villagrá
Associate Professor
Telematics Systems Department
Technical University of Madrid
(DIT-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

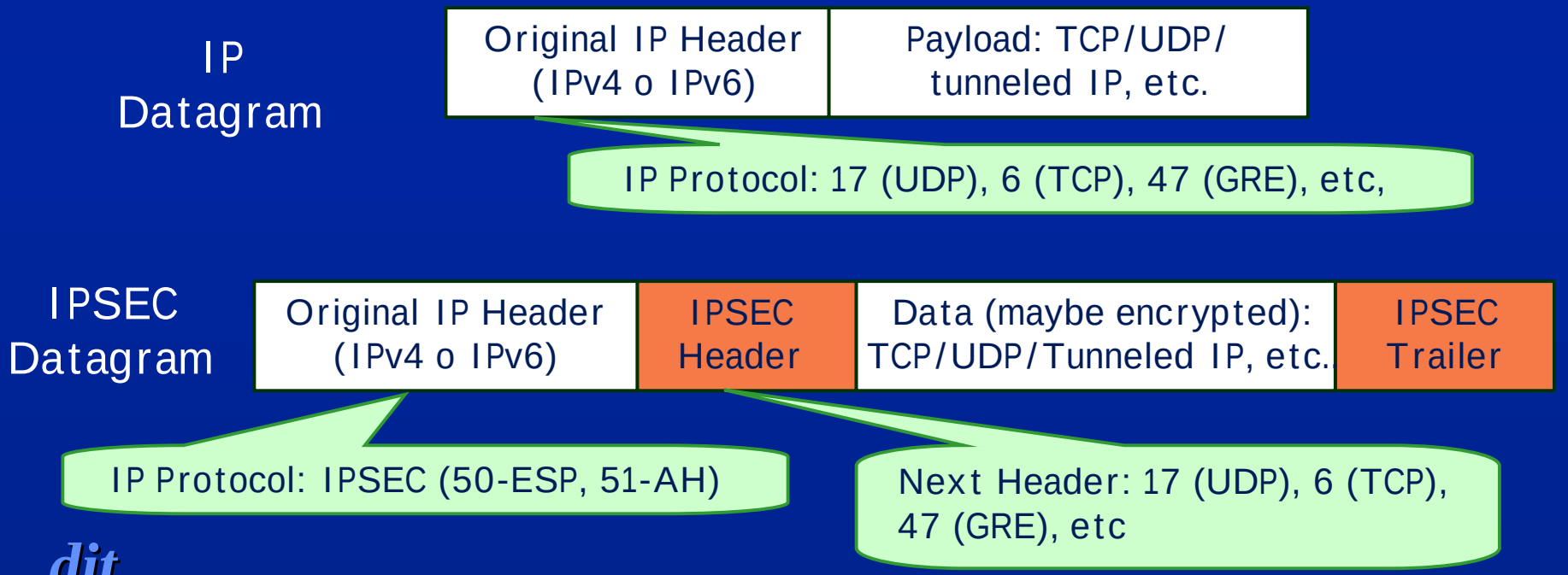
- Two ways to use IPSEC:
  - Transport Mode
    - ✓Directly between remote systems
    - ✓Remote systems must support IPSEC
  - Tunnel Mode
    - ✓Between intermediate systems
    - ✓Secure tunnel for encapsulating the insecure IP datagrams

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



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)
  - Used for identifying the IPSEC use:
    - ✓AH (authentication only)
    - ✓ESP (encryption and optionally authentication)

¿ What is defined by a SA (I) ?

- *Sequence Number Counter*
  - 32 bits value used to generate the sequence number transmitted in the AH and ESP headers
- *Sequence Counter Overflow*
  - Indicates the action to trigger when the sequence number range is over.
- *Anti-Replay Window*
  - Window for limiting the acceptance of valid datagrams
- *AH Information*
  - Authentication algorithms, keys, lifetimes, etc. Used in AH.

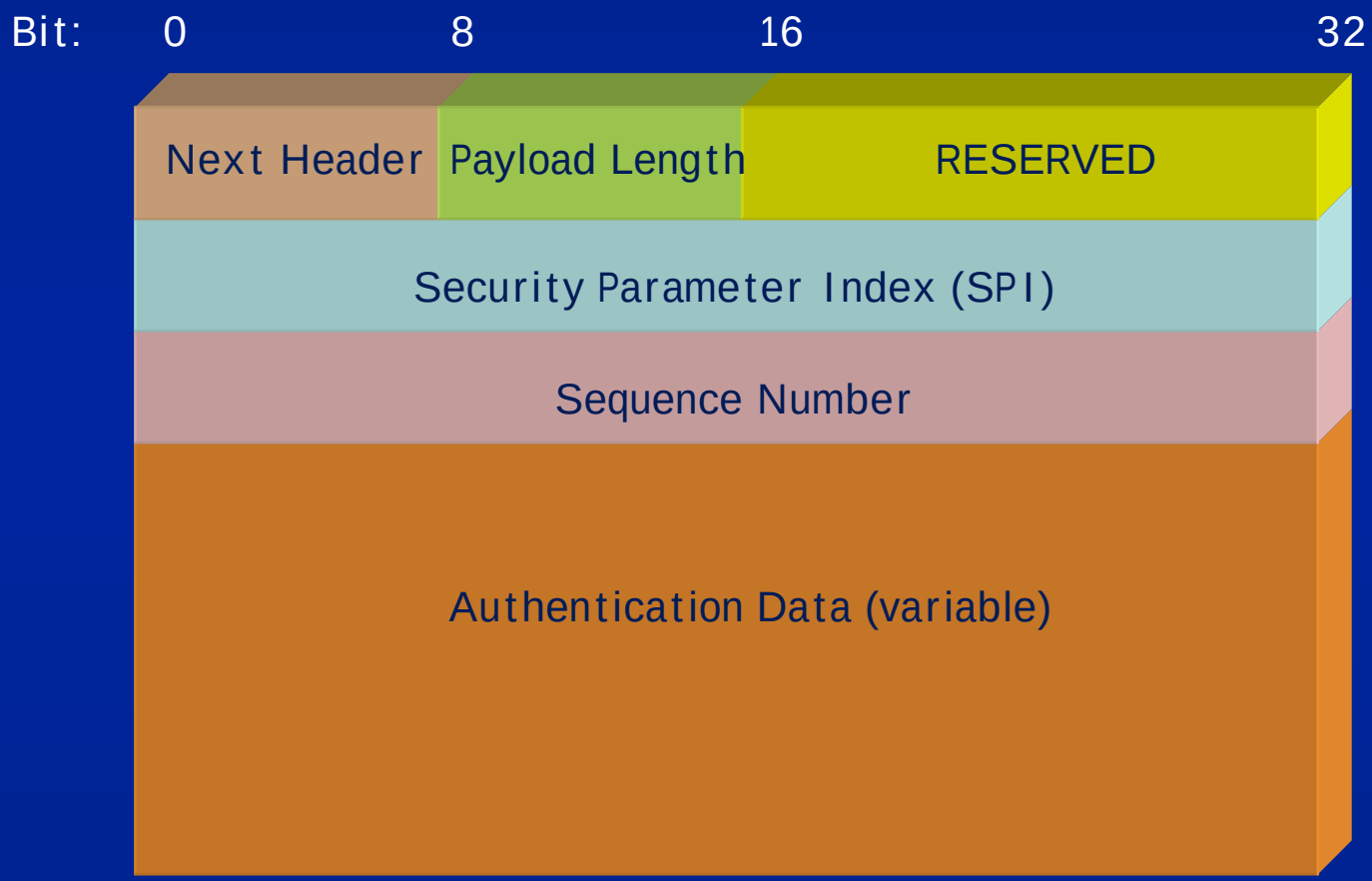
¿ What is defined by a SA (II) ?

- *ESP Information*
  - Authentication and Encrypting algorithms, keys, lifetimes, initial values, etc. Used in 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)



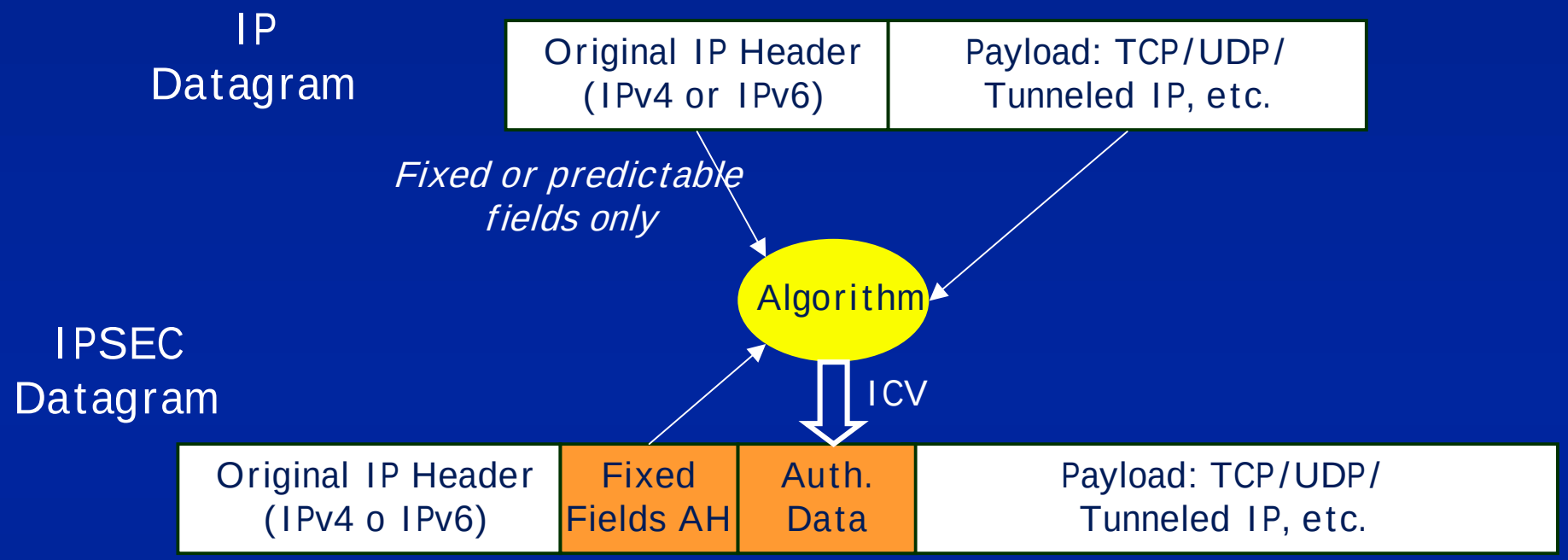
IPSEC Authentication Header

- Next Header: data protocol transmitted inside IP (e.g. TCP, UDP, GRE, etc.)
- Payload Length: Length of the AH header
- Security Parameter Index (SPI): identification of the SA of this datagram
- Sequence Number: counter monotonically incremented with each packer
- Authentication Data: it contains the 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



Non-fixed fields in the IPv4 header

- TOS
- Flags
- Fragment Offset
- TTL
- Header Checksum

Predictable fields in the IPv4 header

- Destination Address

Anti-Replay

- Attack: to replay a valid packet
- Defence: sequence number in AH header
  - Set to 0 when a SA is established
  - With each packet, it is incremented by 1 and transmitted.
  - If it reaches 2^{32}-1, the SA is terminated and another one should be negotiated
- But IP does not ensure neither order nor receipt
  - Receiver has sliding window of size 64
  - It specifies intermediate sequence numbers that the receiver is able to accept.

Encryption Mode: ESP

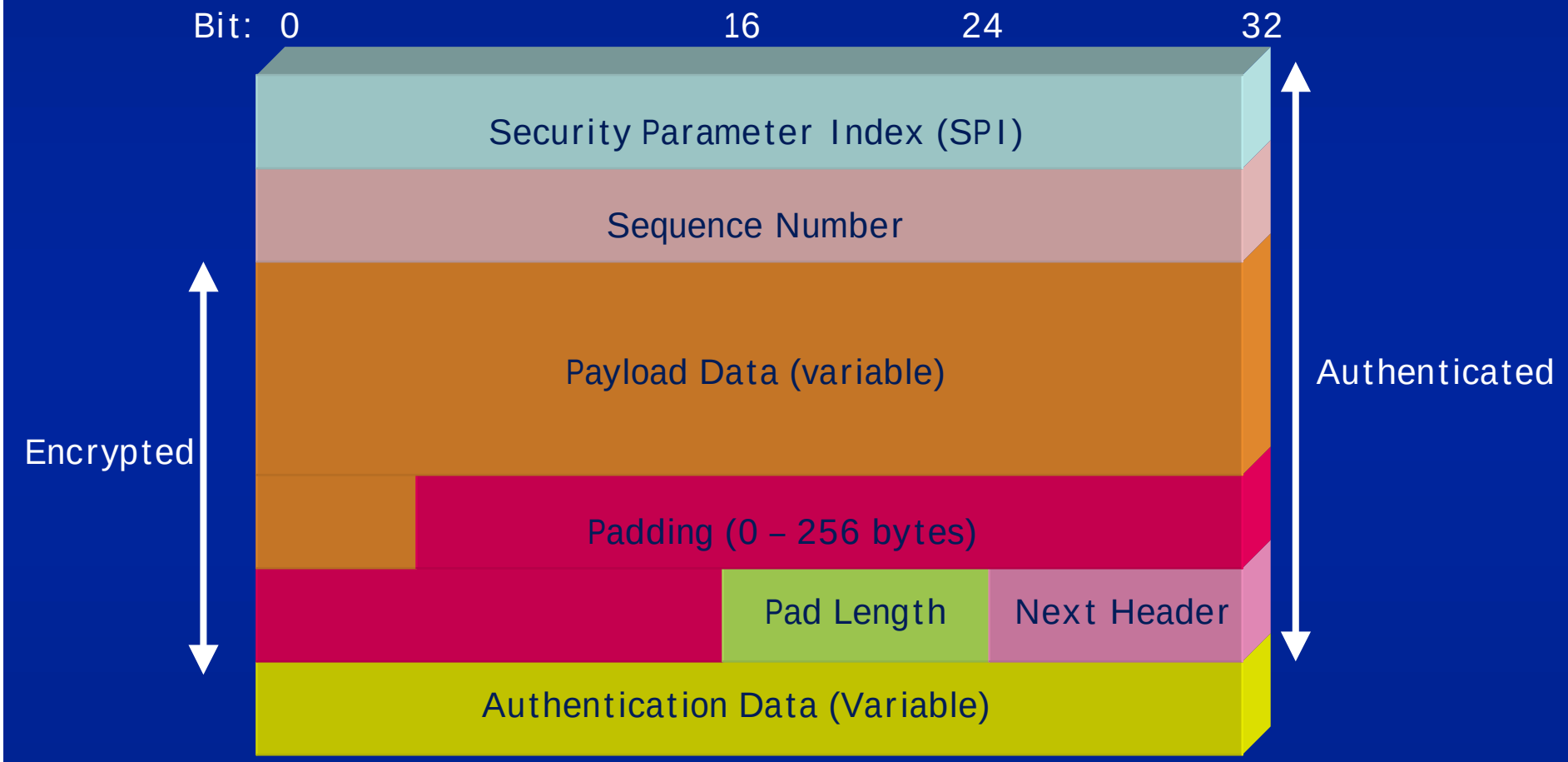
- ESP: Encapsulating Security Payload

- It provides:
  - Content confidentiality
  - Limited traffic flow confidentiality
  - Optionally, authentication services like AH

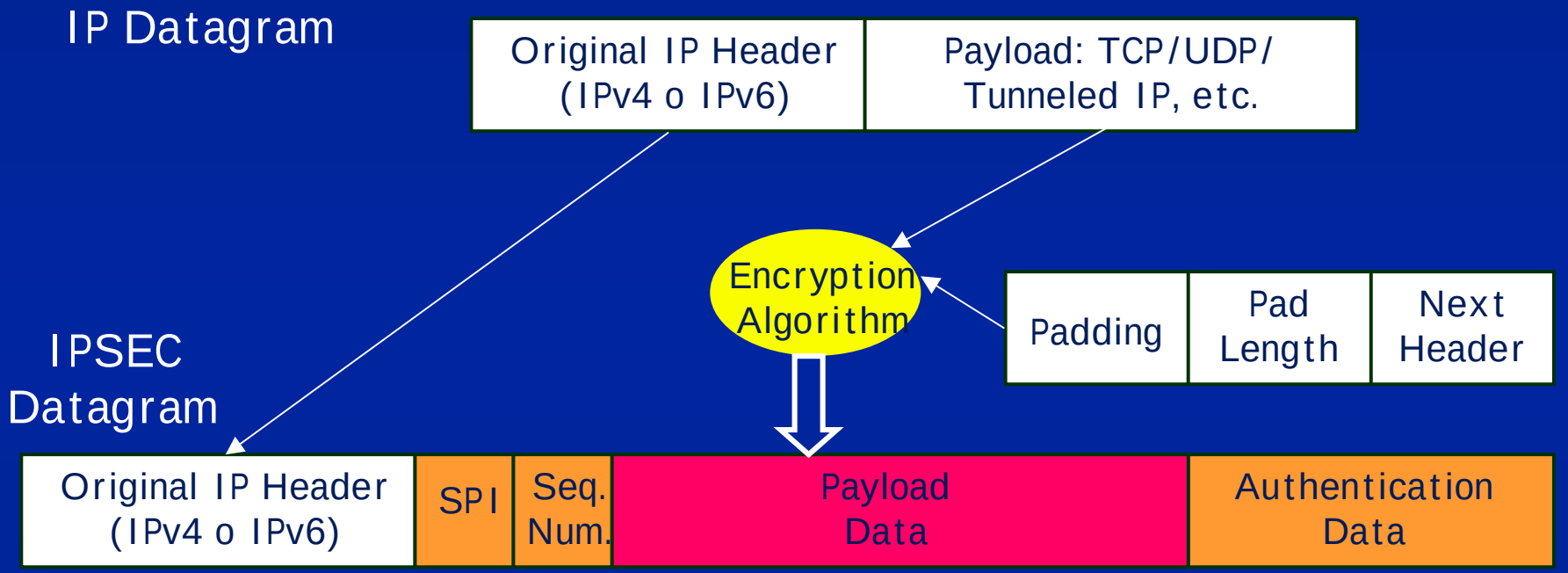
ESP fields

- Security Parameter Index (SPI): identification of the SA of this datagram.
- Sequence Number: counter which is incremented with each packet
- Payload Data: Encrypted data of the IP Protocol
- Padding: Extra bytes needed if the encryption algorithm needs complete text blocks.
- Pad Length: Number of padding bytes
- Next Header: Data protocol in the payload data
- Authentication Data: ICV computed over all the datagram (except Authentication Data field)

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.

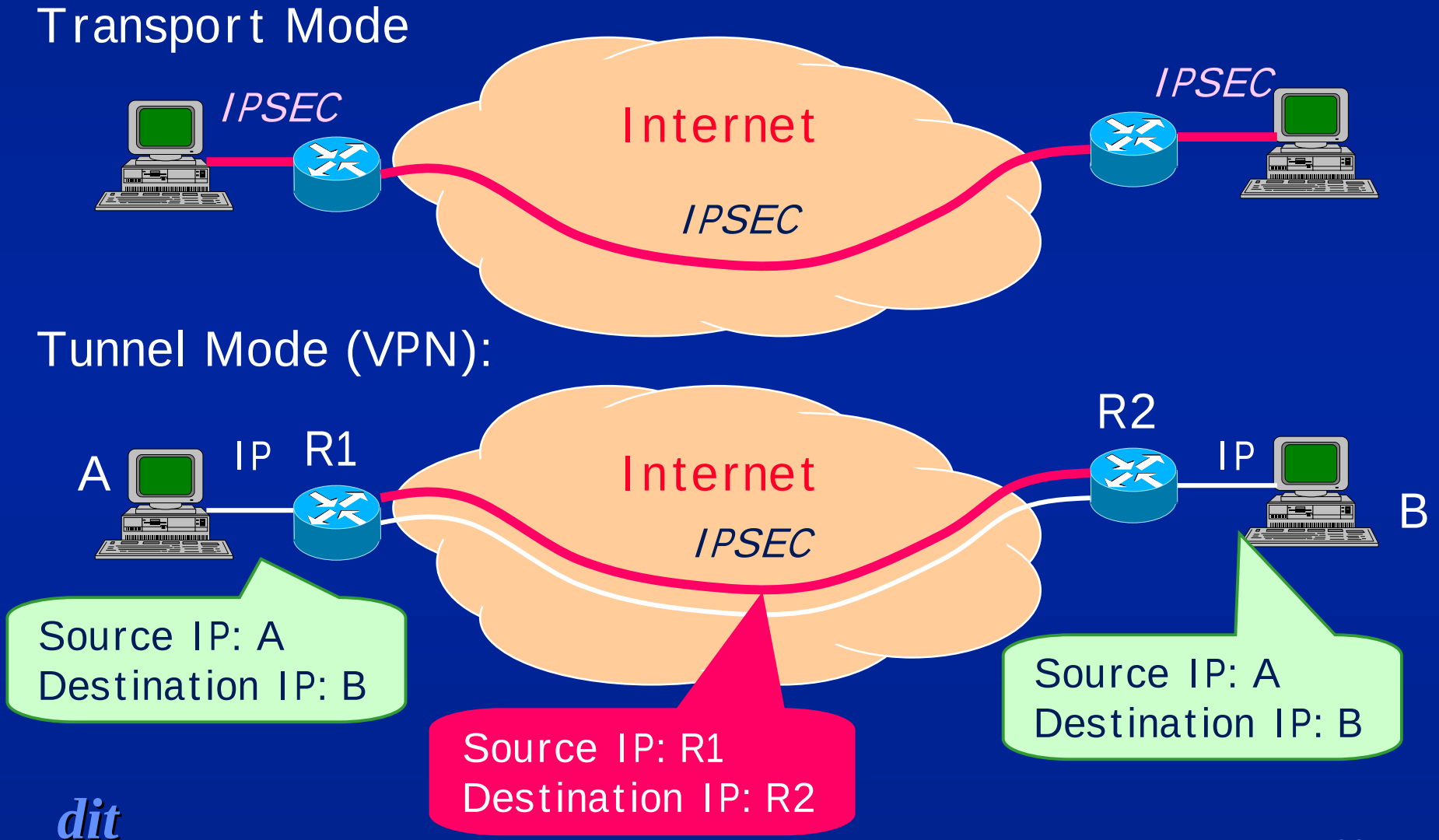
Transport and Tunnel Mode

IP Datagram

IPSEC Datagram
(transport mode)

IPSEC Datagram
(tunnel mode)

Transport and Tunnel Mode



Key Management

- Manual Distribution:
  - Each system is configured with his own keys and with the rest of system's keys
  - Only usable in small and static environments
- Automatic distribution
  - On demand key generation for the SA
  - It is more flexible...
  - But it needs more effort for the configuration and additional software

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 $K=(Y_B)^{X_A} \bmod q=(Y_A)^{X_B} \bmod q$
  - It is modified for authenticating the peers and avoiding the "man-in-the-middle" attack.

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.