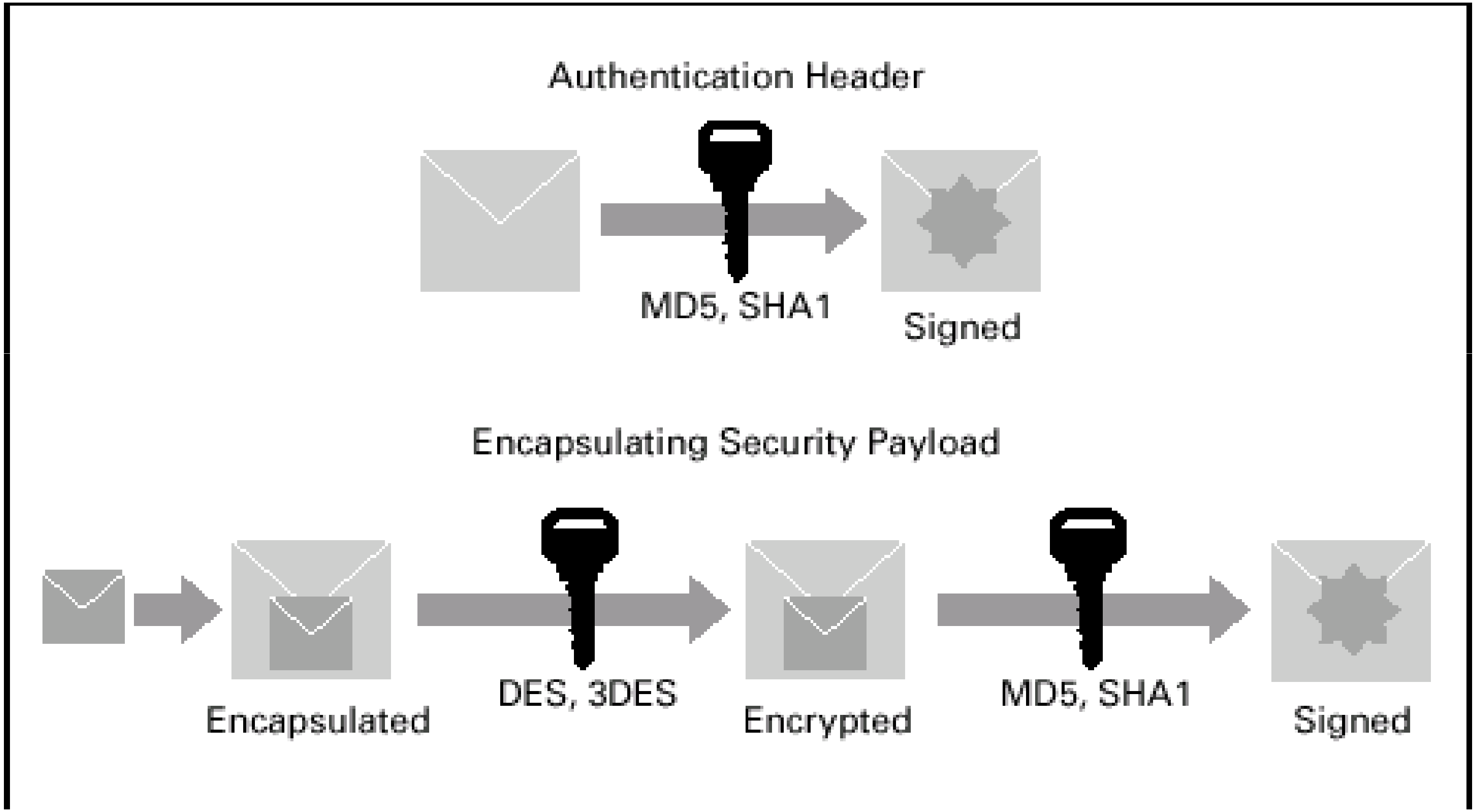
IP Authentication Header
IP ESP

AH & ESP

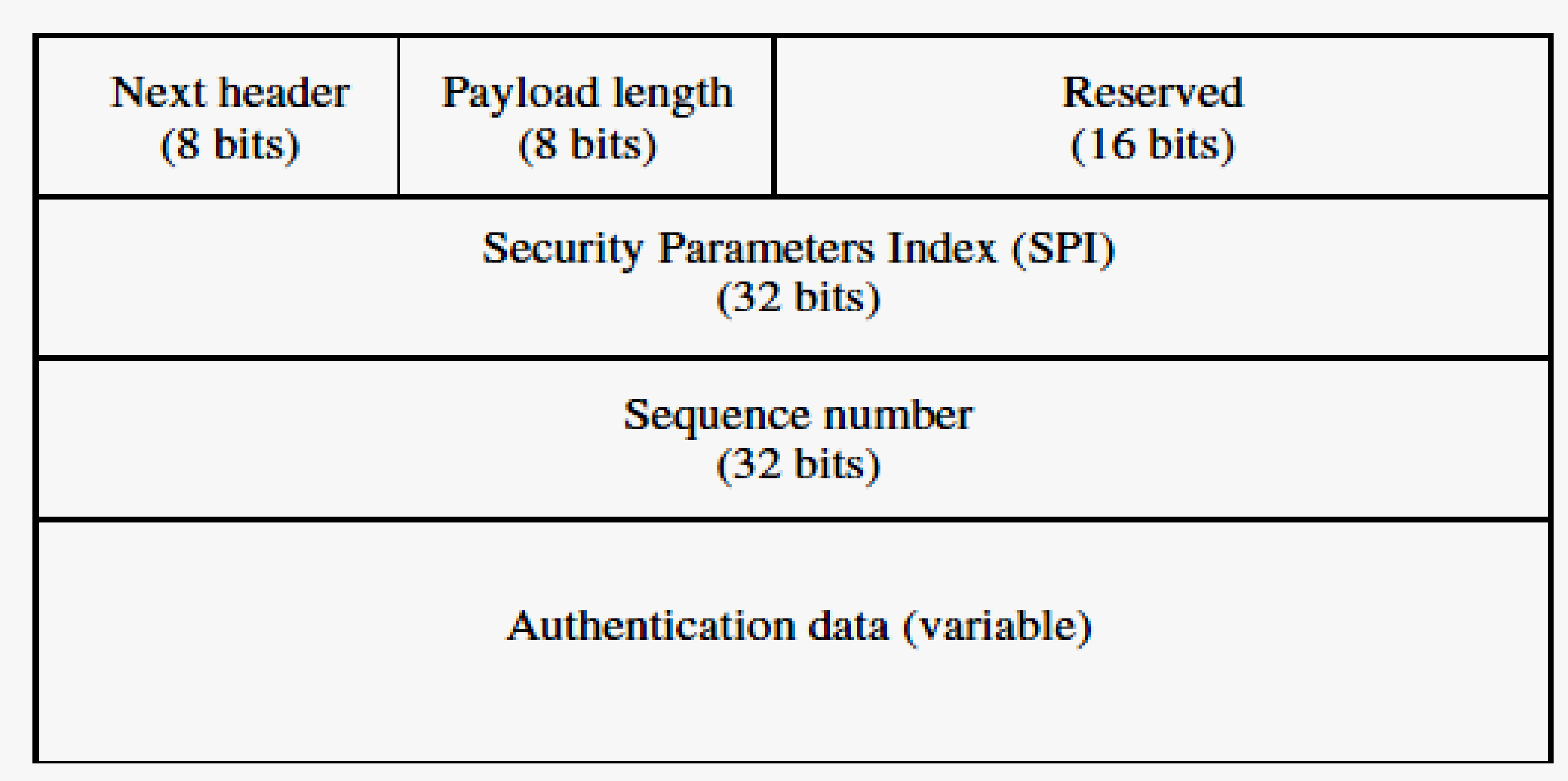

Authentication Header
MD5, SHA1
Signed
Encapsulating Security Payload
Encapsulated
DES, 3DES
Encrypted
MD5, SHA1
Signed

IP Authentication Header

- RFC 1826
- IANA has assigned a protocol number 51 to this protocol
- The protocol field of the outer IP header is set to 51 to indicate that the packet is authenticated
- Provide
  - Data integrity
  - Protection against replays
  - Authentication for IP packets (IP header, upper layer header and data)
    - IP header is not completely authenticated
    - Some IP header fields may change in transit and the sender may not be able to predict the value of these fields when the packet arrives at the receiver
    - Authentication is based on the use of an MAC or the Integrity Check Value (ICV) computation
    - Two hosts must share a secret key
  - Security services between
    - A pair of hosts
    - A pair of security gateway
    - A security gateway and a host
  - key management
    - Manual keying
    - Automated keying via IKE

AH Format

- Six fields

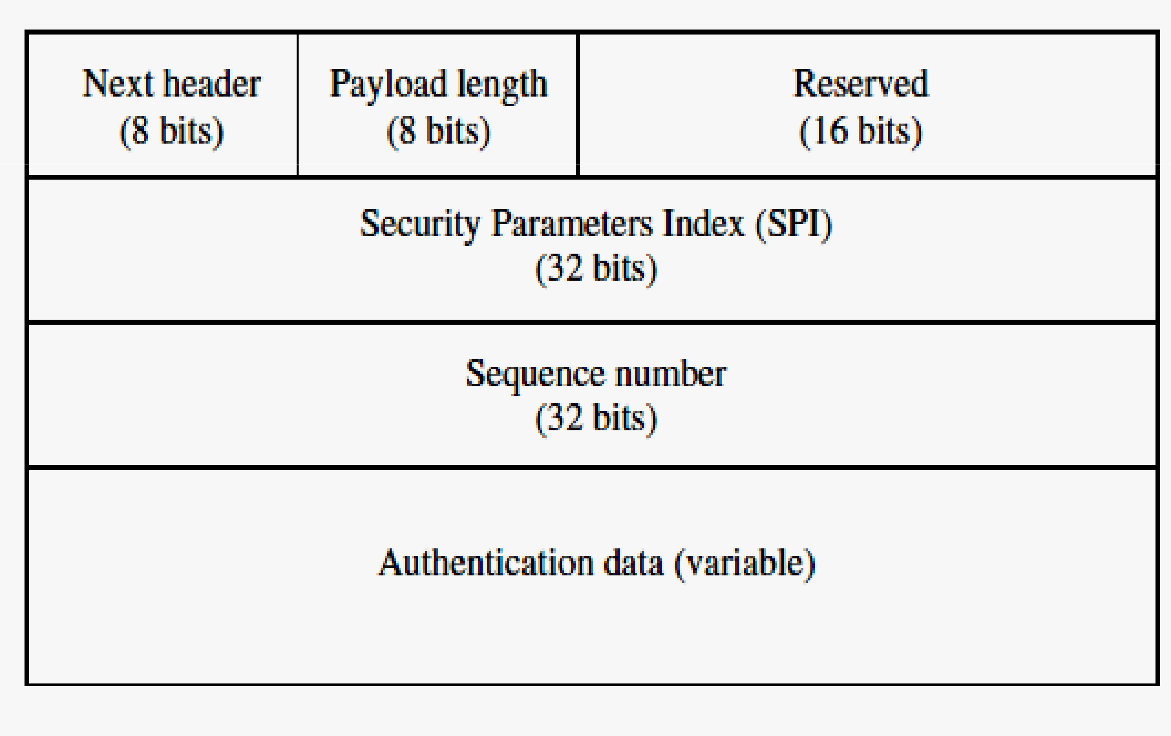


Next header (8 bits)	Payload length (8 bits)	Reserved (16 bits)
Security Parameters Index (SPI) (32 bits)		
Sequence number (32 bits)		
Authentication data (variable)		

Figure 7.4 IPsec AH format.

AH Format

- Size
  - 32 bit for Next header + Payload + Reserved
  - 32 bit for SPI
  - 32 bit for Sequence number
  - 96 = 3*32 bit for Authentication data



Next header (8 bits)	Payload length (8 bits)	Reserved (16 bits)
Security Parameters Index (SPI) (32 bits)		
Sequence number (32 bits)		
Authentication data (variable)		

Figure 7.4 IPsec AH format.

AH Format

- Next header (8 bits):
  - Internet Protocol (IP) number
  - Identifies the type of the next payload after the AH (IP/TCP/UDP)
  - The value is chosen from the set of IP numbers defined in the Internet Assigned Number Authority (IANA)

- Payload length (8 bits):
  - Specifies the length of the AH in 32-bit words, minus 2
  - The default length of the authentication data field is 96 bits

    (three 32-bit words)
  - With a three-word fixed header, there are a total of six words in the header
  - The payload length field: 6-2 = 4

AH Format

- Reserved (16 bits):
  - Reserved for future use
  - It must be set to ‘zero’

- SPI (32 bits):
  - Uniquely identifies the SA for this datagram using Destination IP address and security protocol (AH)
  - SPI values range 1–255 is reserved by the IANA for future use
  - The SPI value of zero (0) is reserved for specific use
    - A key management implementation may use the zero
    - Mean ‘No Security Association Exists’
    - Means SA has not yet been established

Note: Internet Assigned Numbers Authority (IANA)

AH Format

- Sequence number (32 bits):
  - Monotonically increasing counter value - which provides an anti-replay function
  - Initialised to zero when an SA is established
  - The first packet sent using a given SA will have a sequence number ‘1’
  - Even if the sender always transmits this field, the receiver need not act on it

    Processing of the sequence number field is at the discretion of the receiver

- Authentication data (variable):
  - Contains the Integrity Check Value (ICV) or MAC for this packet
  - Field size should be in multiples of 32 bits for IPv4 and 64 bits for IPv6

AH Location

- Employed in the two modes - transport or tunnel modes

Transport mode

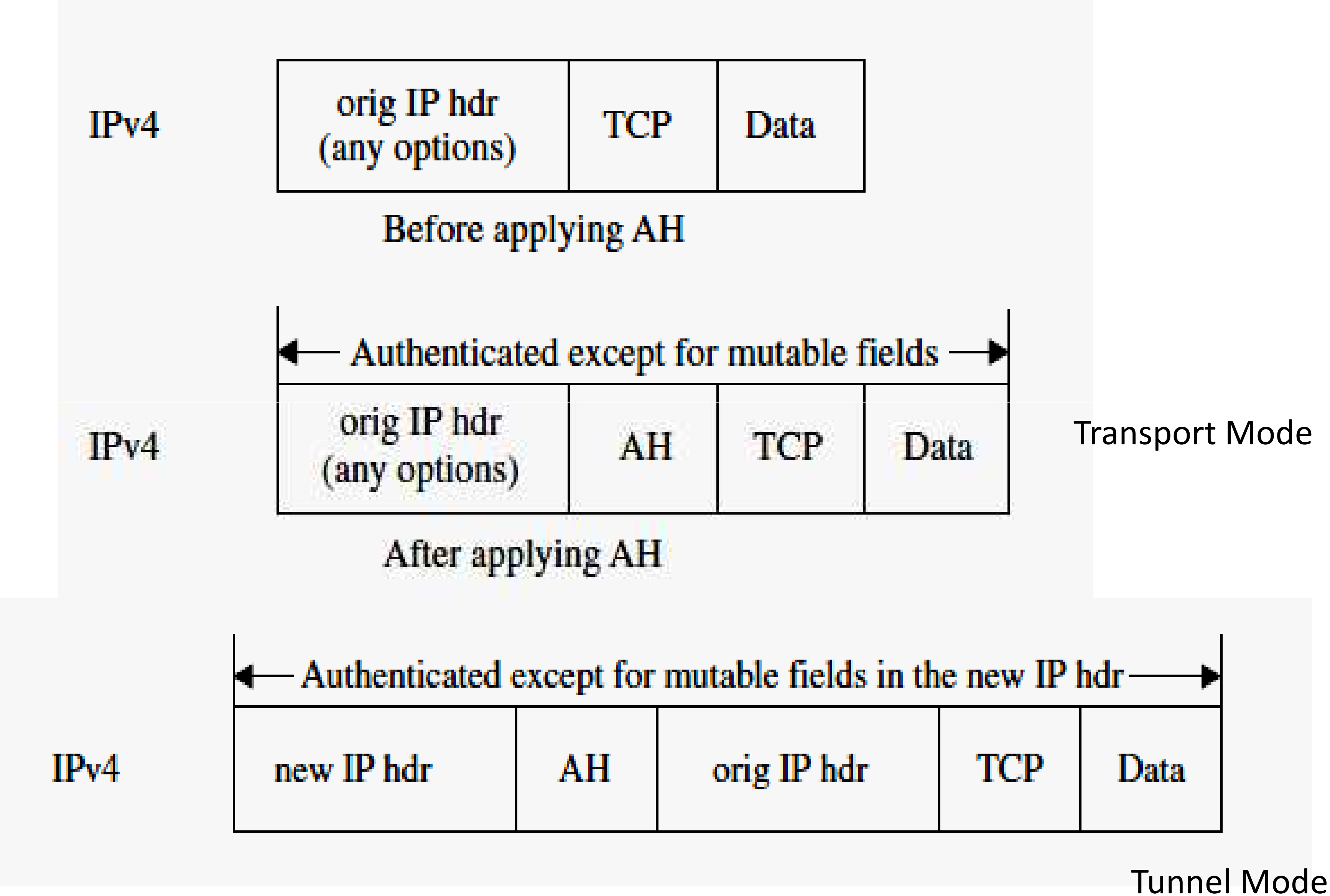
- Applicable only to host implementations
- AH is inserted after the IP header and before an upper layer protocol (TCP, UDP or ICMP), or before any other IPSec header that may have already been inserted
- In the IPv4 context
  - AH is placed after the original IP header and before the upper-layer protocol TCP or UDP.
  - Authentication covers the entire packet, excluding mutable fields in the IPv4 header that are set to zero for MAC computation
- In the IPv6 context
  - AH should appear after hop-to-hop, routing and fragmentation extension headers
  - The destination options extension header(s) could appear either before or after AH, depending on the semantics desired
  - Authentication again covers the entire packet, excluding mutable fields that are set to zero for MAC computation

AH Location

Tunnel mode

- AH can be employed in either hosts or security gateways
- Inner IP header carries the ultimate source and destination addresses
- Outer IP header may contain different IP addresses (i.e. addresses of firewalls or other security gateways)
- AH protects the entire inner IP packet, including the entire inner IP header
- The position of AH in tunnel mode, relative to the outer IP header, is the same as for AH in transport mode

AH Location



IPv4

orig IP hdr (any options)	TCP	Data

Before applying AH

← Authenticated except for mutable fields →

IPv4

orig IP hdr (any options)	AH	TCP	Data

After applying AH

Transport Mode

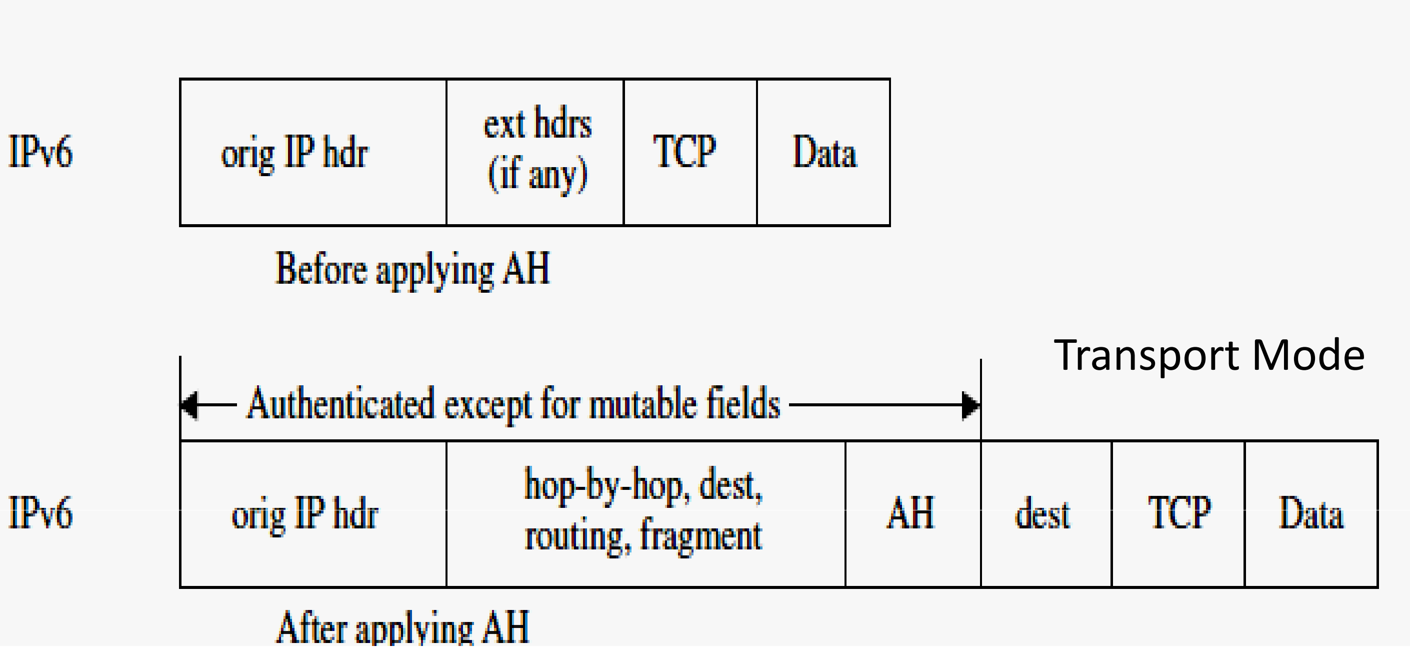
← Authenticated except for mutable fields in the new IP hdr →

IPv4

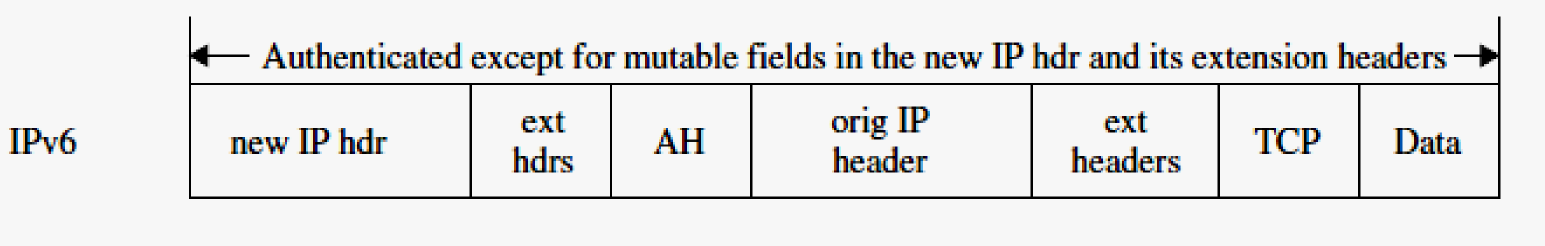
new IP hdr	AH	orig IP hdr	TCP	Data

Tunnel Mode

AH Location



Transport Mode


Authenticated except for mutable fields in the new IP hdr and its extension headers
IPv6
new IP hdr
ext hdrs
AH
orig IP header
ext headers
TCP
Data

(c) AH tunnel mode for typical IPv4 and IPv6 packets

Tunnel Mode

IP ESP

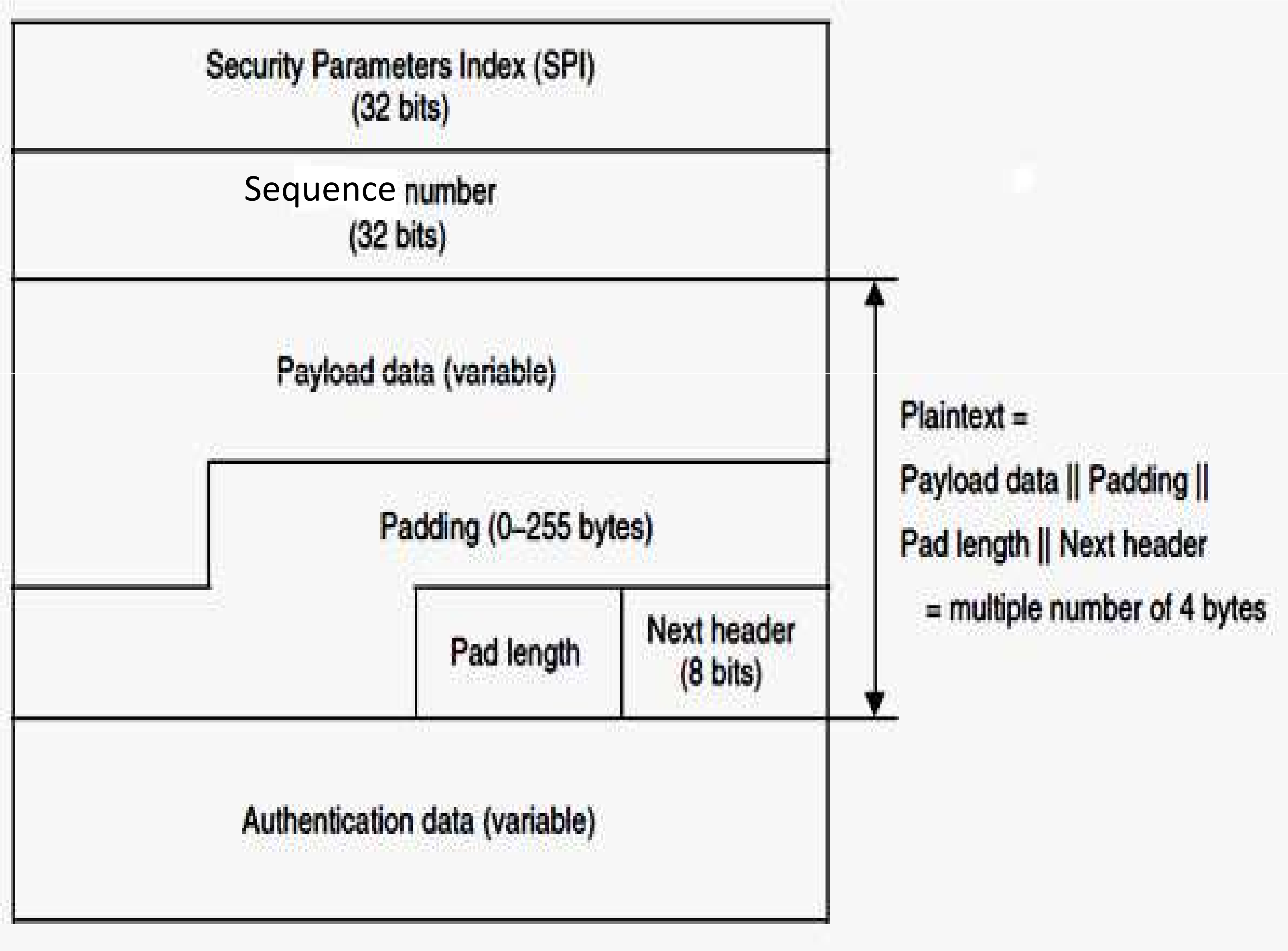
- RFC 2406
- IANA – assigned protocol number is 50
- The protocol field of the outer IP header is set to 50 to indicate that the packet is an ESP packet

- Provides
  - Confidentiality
  - Data authentication
  - Integrity
  - Anti-replay service
  - Limited traffic flow confidentiality

  - Security services between
    - A pair of hosts
    - A pair of security gateway
    - A security gateway and a host

  - key management
    - Manual keying
    - Automated keying via IKE

ESP Packet Format



Security Parameters Index (SPI) (32 bits)

Sequence number (32 bits)

Payload data (variable)

Padding (0–255 bytes)

Pad length

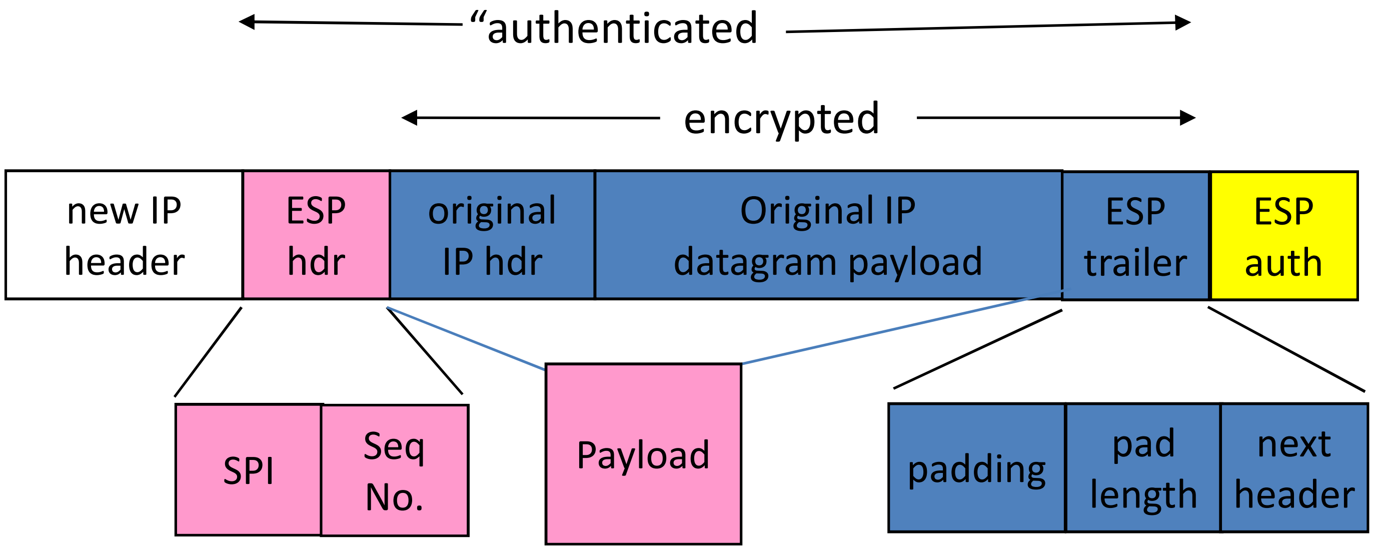
Next header (8 bits)

Authentication data (variable)

Plaintext =
Payload data || Padding ||
Pad length || Next header
= multiple number of 4 bytes

ESP Packet Format

Tunnel mode packet details



ESP Packet Format

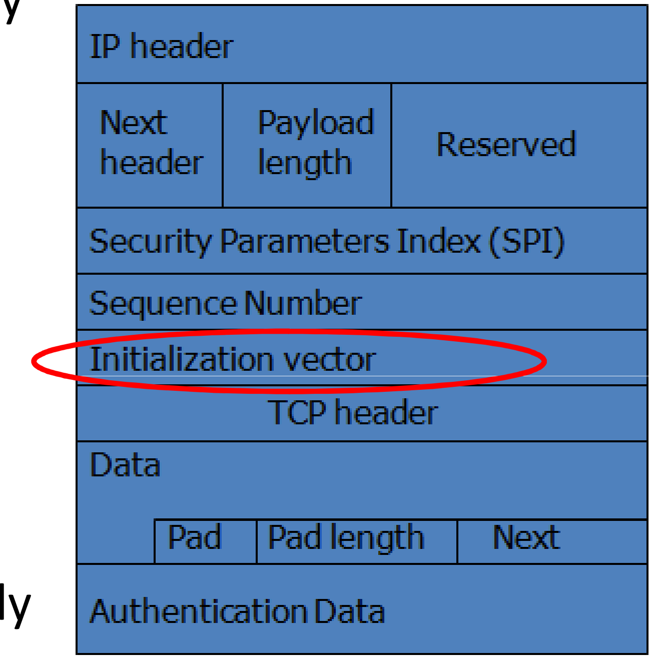
- SPI (32 bits):
  - uniquely identifies an SA for this datagram
  - Mandatory and always present

- Sequence number (32 bits):
  - Monotonically increasing counter value
  - Provides an anti-replay function
  - Mandatory

- Payload data (variable):
  - Variable-length field
  - Contains data described by the next header field
  - Length in bytes
  - Initialisation vector (IV) may be carried explicitly in the payload field is required

ESP Packet Format

- Padding (variable):
  - Used to fill the plaintext to the size required by the algorithm - on a 32-bit boundary
  - The sender may add 0–255 bytes of padding
  - Padding is applied next to the payload data
  - The plaintext consists of the IV, payload data (padded), payload length, next header
- Pad length (8 bit):
  - Indicates the number of pad bytes immediately preceding it
  - The range of valid values is 0–255, where a value of 0 indicates that no padding
  - Mandatory



ESP Packet Format

- Next header (8 bits):
  - This field identifies the type of data contained in the payload data field
  - The value of this field is chosen from the set of IP numbers defined by the IANA
  - Mandatory field

- Authentication data (variable):
  - Containing an ICV (**Integrity Check Value)**
  - Computed over the ESP packet minus the authentication data
  - Optional field, included only if the authentication service has been selected for the SA
  - The authentication algorithm must specify the length of the ICV and the comparison rules and processing steps for validation

ESP Header Location

- Employed in the two transport or tunnel modes

Transport mode

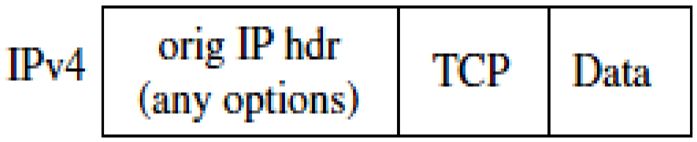
- Applicable only to host implementations
- provides protection for upper protocols, but not the IP header
- ESP is inserted after the IP header and before an upper-layer protocol (TCP, UDP or ICMP), or before any other IPsec headers that have already been inserted
- In the IPv4 context
  - ESP is placed after the IP header, but before the upper-layer protocol
  - *The ESP trailer encompasses any padding, plus the* pad length, and next header fields
- In the IPv6 context
  - ESP appears after hop-by-hop, routing and fragmentation extension headers
  - The destination options extension header(s) could appear either before or after the ESP header depending on the semantics desired, still generally desirable to place the destination options header(s) after the ESP header

ESP Header Location

Tunnel mode

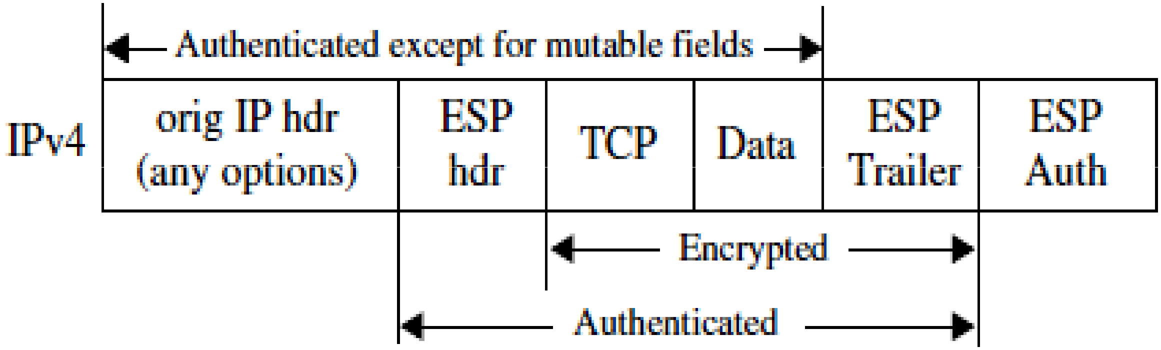
- Employed in either hosts or security gateways
- Inner IP header carries the ultimate source and destination addresses, while an outer IP header may contain different IP addresses such as addresses of security gateways
- Protects the entire inner IP packet, including the entire inner IP header

ESP Header Location



IPv4	orig IP hdr (any options)	TCP	Data

Before applying ESP



← Authenticated except for mutable fields →

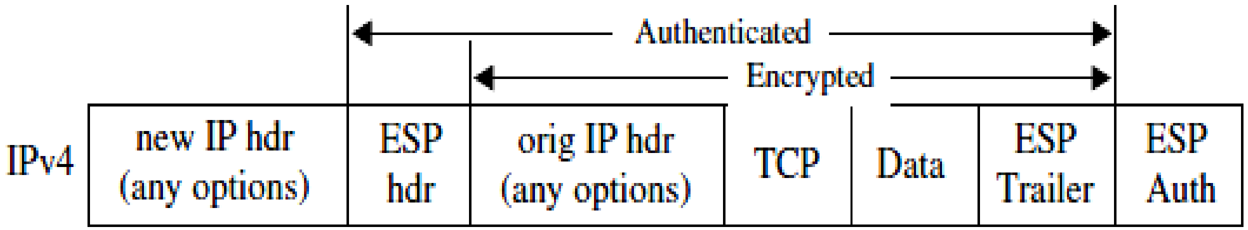
IPv4	orig IP hdr (any options)	ESP hdr	TCP	Data	ESP Trailer	ESP Auth

← Encrypted →

← Authenticated →

Transport Mode

After applying ESP



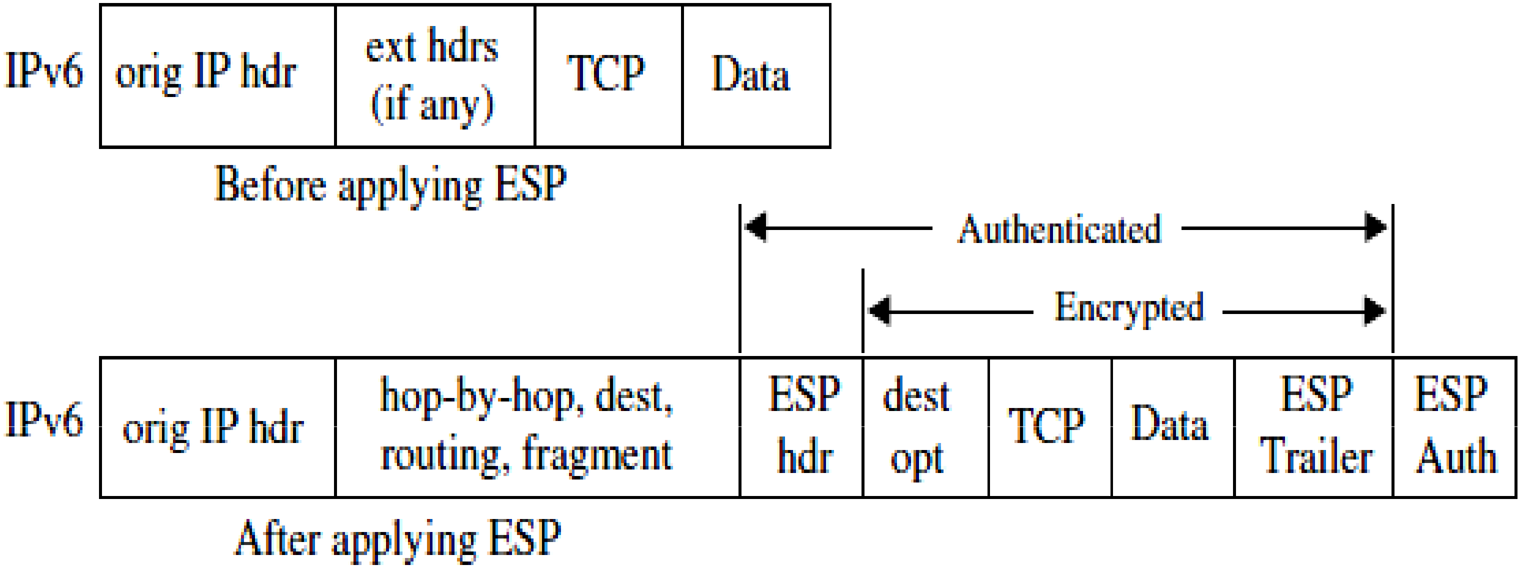
← Authenticated →

← Encrypted →

IPv4	new IP hdr (any options)	ESP hdr	orig IP hdr (any options)	TCP	Data	ESP Trailer	ESP Auth

Tunnel Mode

ESP Header Location



IPv6	orig IP hdr	ext hdrs (if any)	TCP	Data

Before applying ESP

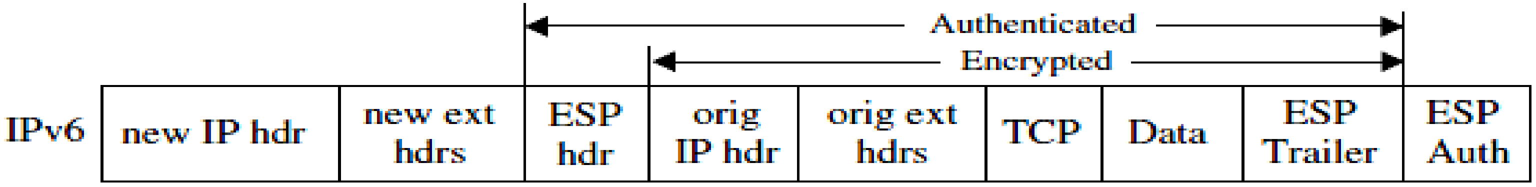
Authenticated

Encrypted

IPv6	orig IP hdr	hop-by-hop, dest, routing, fragment	ESP hdr	dest opt	TCP	Data	ESP Trailer	ESP Auth

After applying ESP

Transport Mode



Authenticated

Encrypted

IPv6	new IP hdr	new ext hdrs	ESP hdr	orig IP hdr	orig ext hdrs	TCP	Data	ESP Trailer	ESP Auth

(c) ESP tunnel mode for typical IPv4 and IPv6 packets

Tunnel Mode

Encryption and Authentication Algorithms

- The encryption authentication algorithm employed is specified by the SA

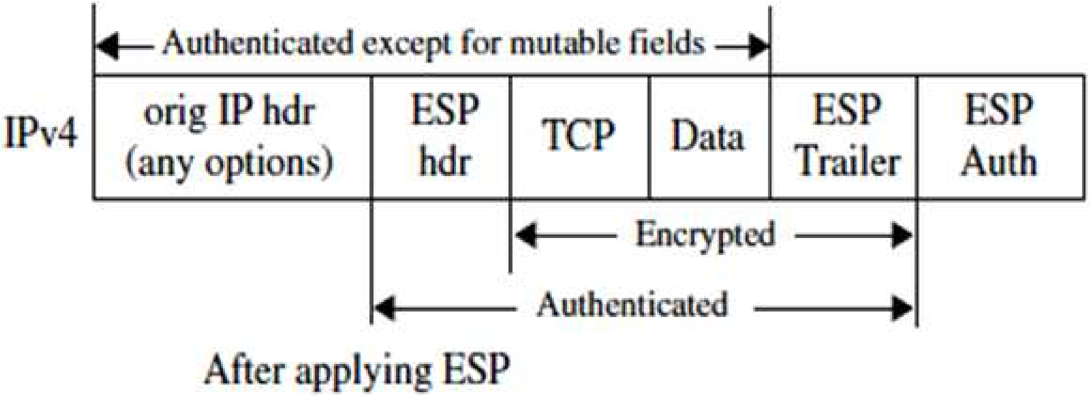
1. *Encryption*
2. *Decryption*
3. *Authentication*
4. *ICV*

Encryption and Authentication Algorithms

1. Encryption
   - ESP is designed for use with symmetric algorithms like a triple DES in CBC mode
   - Number of other algorithms have been assigned identifiers in the DOI document
   - These algorithms for encryption are: RC5, IDEA, CAST and Blowfish
   - Payload data, padding, pad length and next header are encrypted
   - Done using- the key, encryption algorithm, algorithm mode (block or stream) and an IV - indicated by the SA

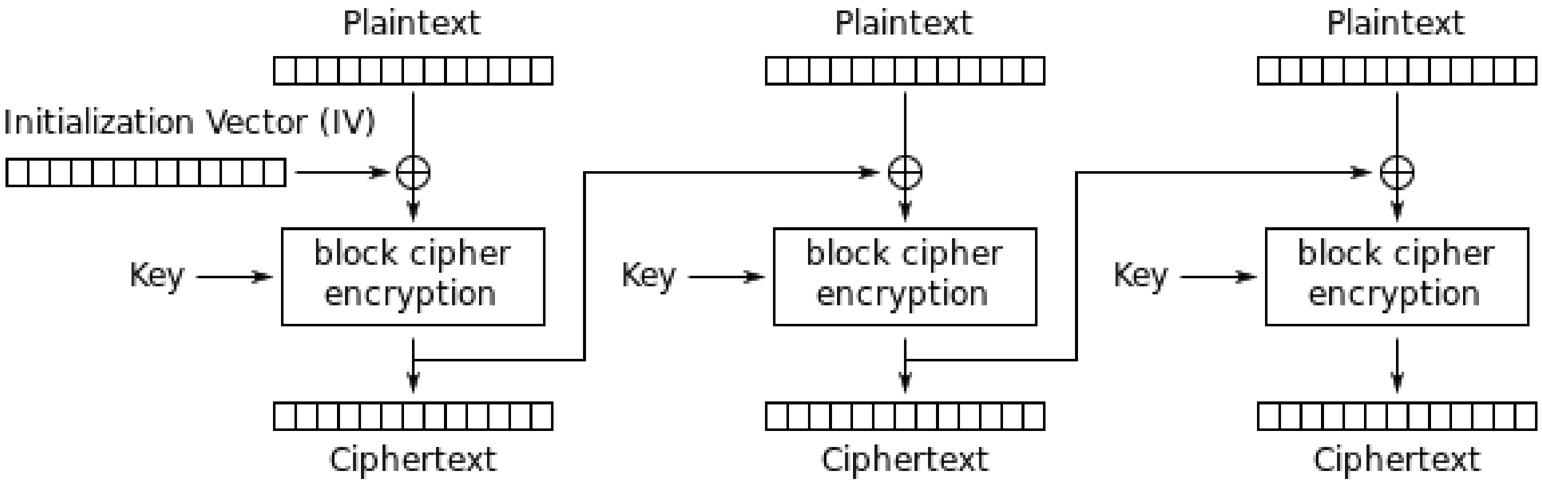
Encryption and Authentication Algorithms

1. Encryption
   - Encryption is performed before the authentication
   - ESP payload does not encompass the authentication data field
   - This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver, prior to decrypting the packet
   - It will reduce the impact of service attacks
   - At the receiver, parallel processing of packets is possible because decryption can take place in parallel with authentication
   - Since the authentication data is not protected by encryption, a keyed authentication algorithm must be employed to compute the ICV

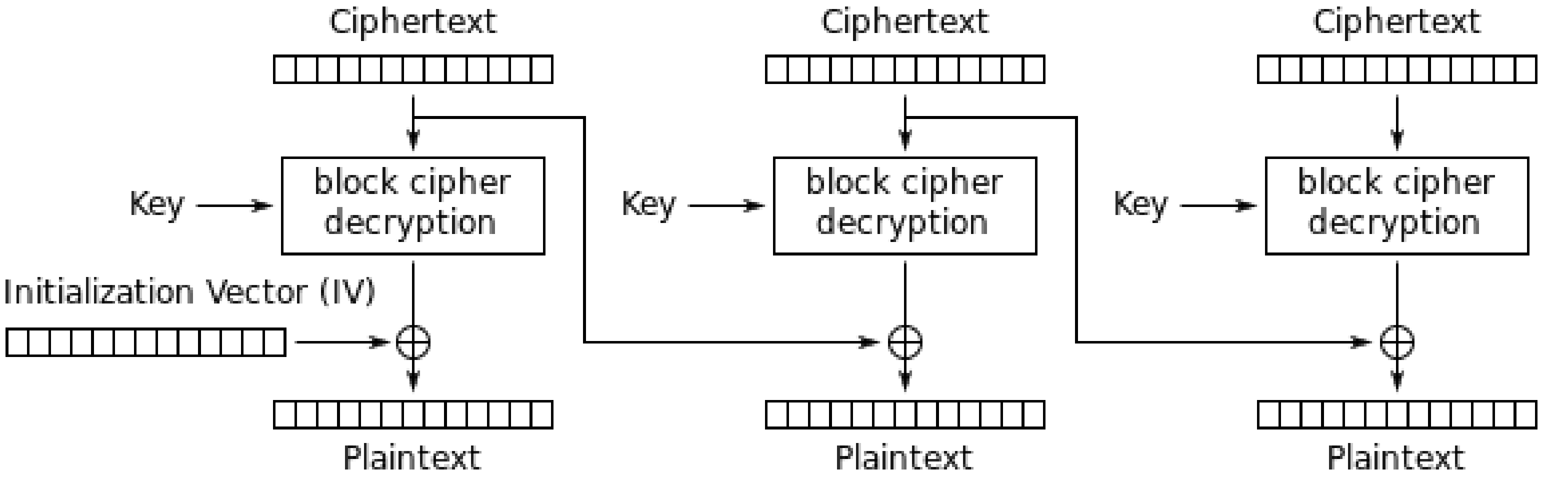


Encryption and Authentication Algorithms

1. Encryption
   - 3DES–CBC mode requires an IV that is the same size as the block size
   - The IV is XORed with the first plaintext block before it is encrypted
   - For successive blocks, the previous ciphertext block is XORed with the current plaintext before it is encrypted
   - Triple DES, known as DES–EDE3, processes each block three times, each time with a different key
   - Therefore, the triple DES algorithm has 48 rounds (3*16)
   - In DES–EDE3-CBC, an IV is XORed with the first 64-bit plaintext block (P1)
   - Key size
     - Variable-sized key (RC5)
     - Specific key size (DES, IDEA)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

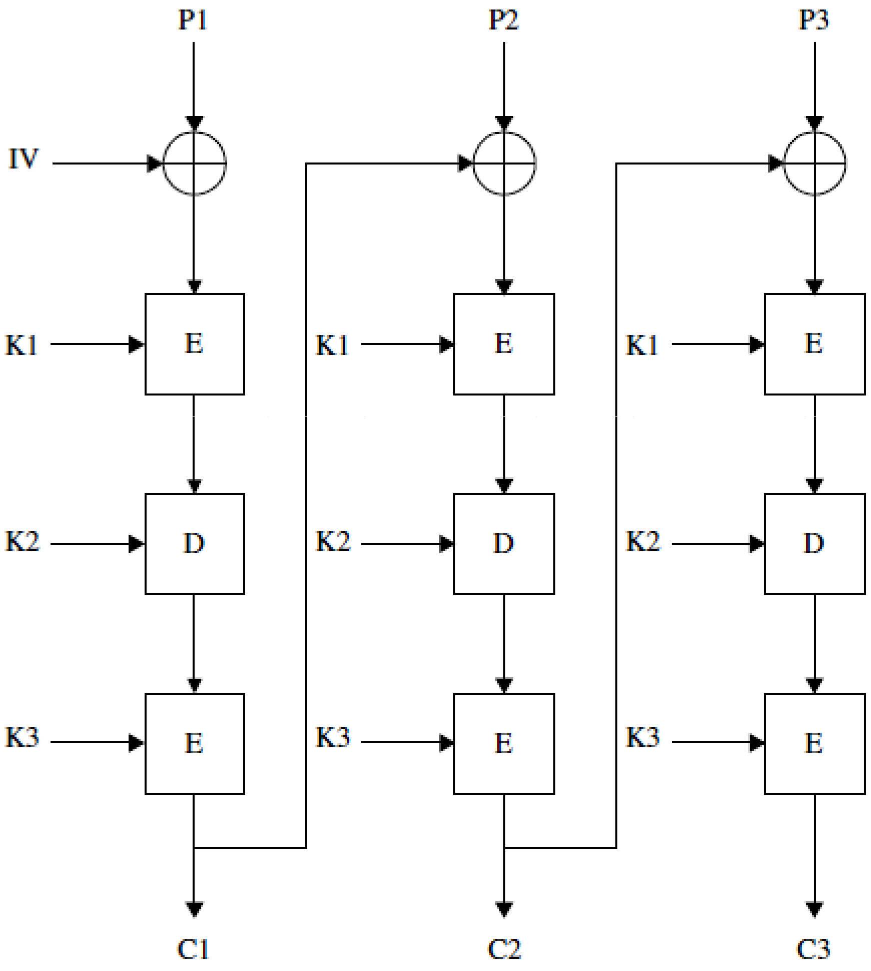


Figure 7.8 DES–EDE3–CBC algorithm.

Encryption and Authentication Algorithms

2. Decryption

- The receiver
  - Decrypts
    - ESP payload data
    - Padding
    - Pad length
    - Next header
  - Using
    - Key
    - Encryption algorithm
    - Algorithm mode
    - IV data
      - Explicit IV data is indicated – IV taken from the payload field and input to the decryption algorithm
      - Implicit IV data is indicated - a local version of the IV is constructed and input to the decryption algorithm

Encryption and Authentication Algorithms

2. Decryption

- Steps for reconstructing the original datagram depend
  - The mode (transport or tunnel)
  - Description in the Security Architecture document

- Padding processed as given in the encryption algorithm
- If authentication has been computed, verification and decryption are performed serially or in parallel
  - If performed serially, then ICV or MAC verification should be performed first
  - If performed in parallel, verification must be completed before the decrypted packet is passed on for further processing
  - The order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver

Encryption and Authentication Algorithms

3. Authentication

- The authentication algorithm employed is specified by the SA
- Message Authentication Codes (MACs) based on
  - Symmetric encryption algorithms (i.e. DES)
  - On one-way hash function (i.e. MD5 or SHA-1)
- Done on payload data, padding, pad length and next header

Encryption and Authentication Algorithms

4. ICV

- MAC value produced by an MAC algorithm
- Sender computes the ICV over the ESP packet minus the authentication data
- As with AH, ESP supports the use of an MAC with a default length of 96 bits
- The current specification for use of the HMAC computation must support:
  - HMAC–MD5–96
  - HMAC–SHA-1–96