# CYBER FORENSICS
# CS6004

# Syllabus

UNIT I NETWORK LAYER SECURITY & TRANSPORT LAYER SECURITY

UNIT II E-MAIL SECURITY & FIREWALLS

UNIT III INTRODUCTION TO COMPUTER FORENSICS

UNIT IV EVIDENCE COLLECTION AND FORENSICS TOOLS

UNIT V ANALYSIS AND VALIDATION

# UNIT I

## NETWORK LAYER SECURITY
## &
## TRANSPORT LAYER SECURITY

Network layer security:

- IPSec Protocol
- IP Authentication Header
- IP ESP
- Key Management Protocol for IPSec

Transport layer Security:

- SSL protocol
- Cryptographic Computations
- TLS Protocol

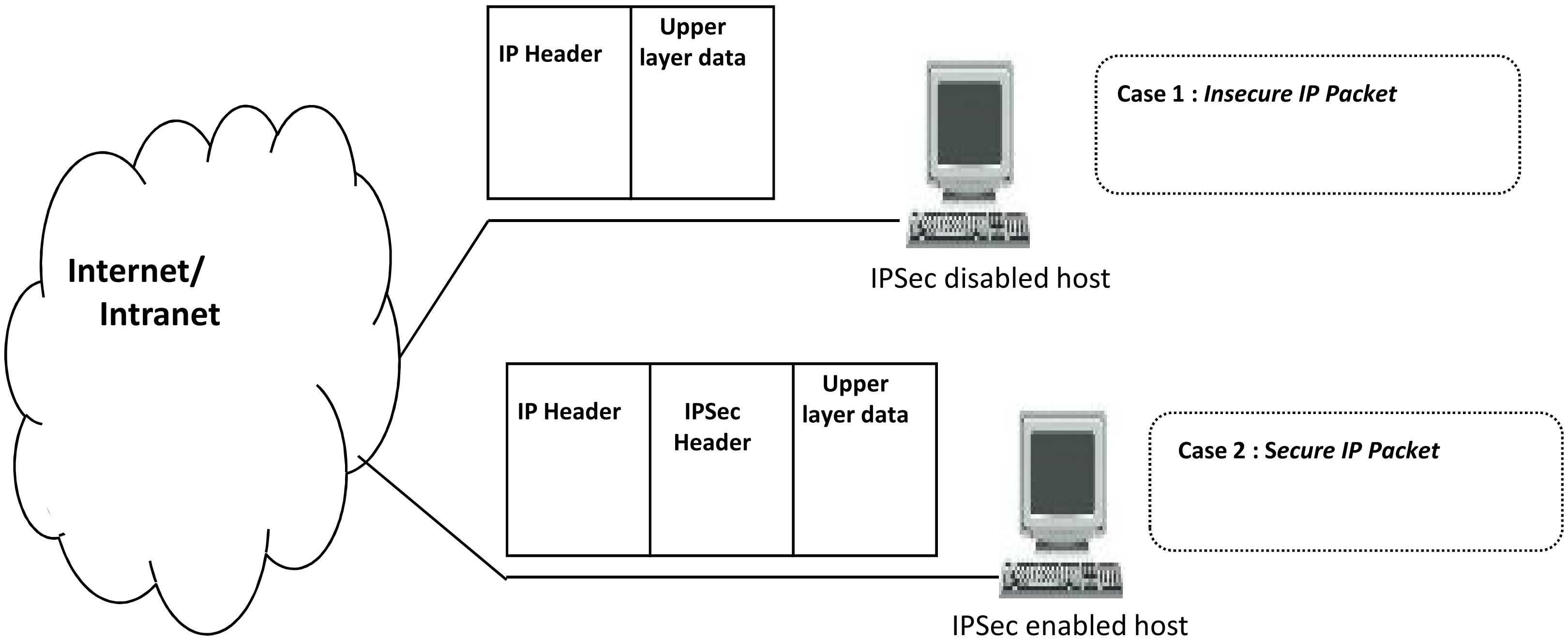
# Network Layer Security :
## IPSec Protocol

IPSec Protocol Documents
Security Associations (SAs)
Hashed Message Authentication Code (HMAC)

# IPSec Protocol

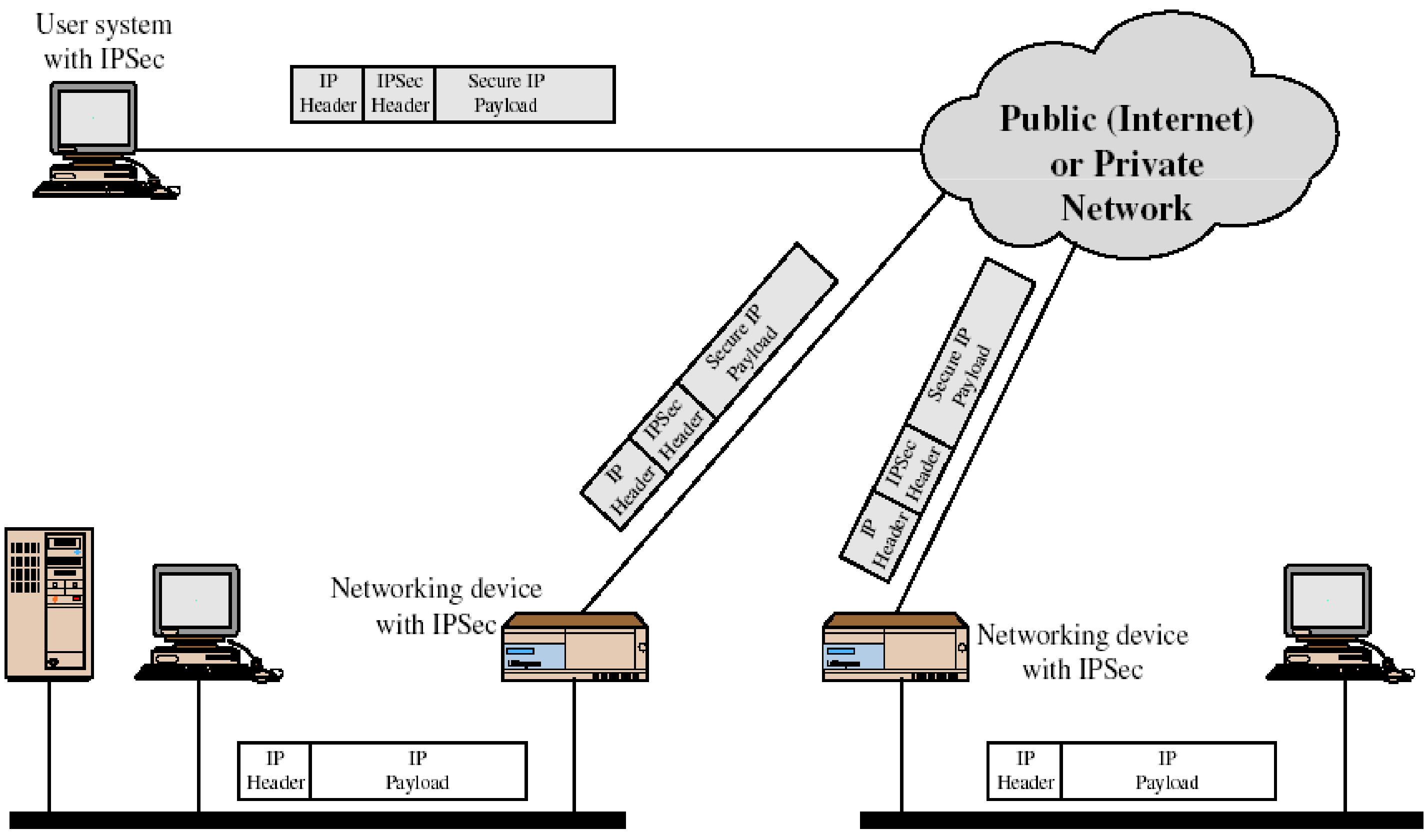
- Designed to protect communication
- It is a set of security extensions
- Developed by the IETF (**Internet Engineering Task Force)**
- It provides privacy and authentication services at the IP layer by using modern cryptography

# IPSec Protocol



# IPSec Protocol

- Operates in a host or a security gateway environment
- The protection offered is based on requirements defined by a Security Policy Database (SPD)
- SPD is established and maintained by a user or system administrator



# IPSec Protocol

- Network Layer / IP Layer - IP datagram - is protected using IPSec protocol
- Two main transformation of IPSec
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- AH and ESP –protocols provide
  - Connectionless integrity - accuracy
  - Data origin authentication
  - Confidentiality - privacy
  - Anti-replay service – intercept and insert packets
  - Access control
- AH and ESP may be applied alone or in combination
- They are configured in a data structure called a Security Association (SA)

# IPSec Protocol

- Two modes of operations
- Transport mode
  - Provides Peer to Peer communication security (between host)
  - Provides protection for upper-layer protocol data units (PDUs)
    - TCP packet
    - UDP segment
    - Internet Control Message Protocol (ICMP) packet
  - Data protected but header left in clear
- Tunnel mode
  - Used by network routers to protect IP datagram's passing across insecure network
  - Provides protection for entire IP datagram's
  - Add new header for next hop
  - Good for VPNs, gateway to gateway security

# IPSec Modes of Operation

Original IP Datagram

| | | |
|---|---|---|
| **IP Header** | **TCP Header** | **Data** |

- Transport Mode: protect the upper layer protocols

Transport Mode protected packet

| | | | |
|---|---|---|---|
| **IP Header** | **IPSec Header** | **TCP Header** | **Data** |

*protected*

- Tunnel Mode: protect the entire IP payload

Tunnel Mode protected packet

| | | | | |
|---|---|---|---|---|
| **New IP Header** | **IPSec Header** | **Original IP Header** | **TCP Header** | **Data** |

*protected*

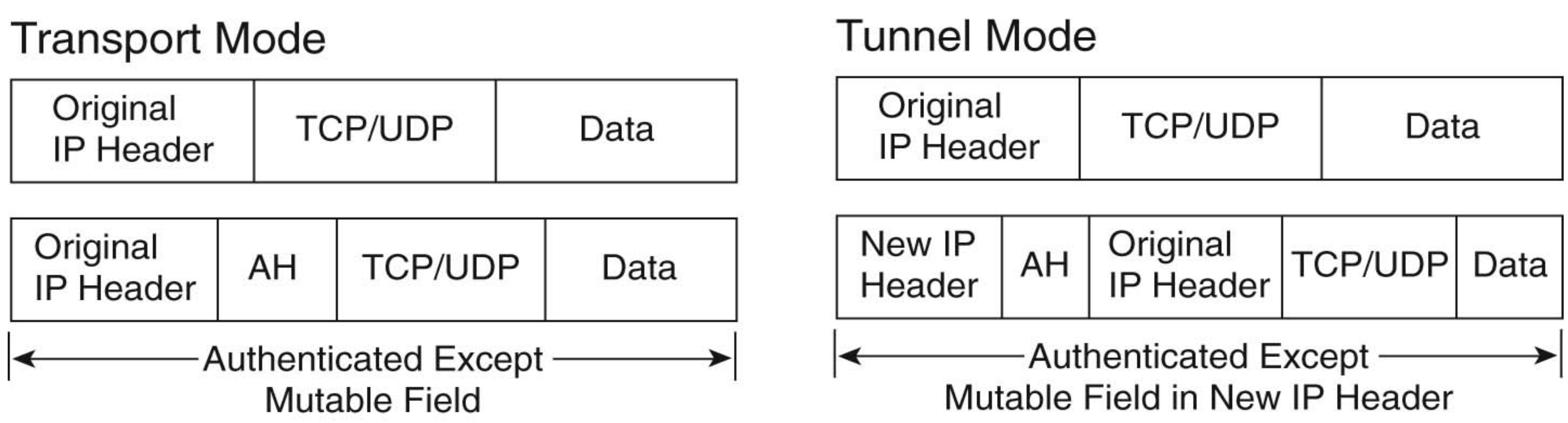
# IPSec Modes of Operation-AH

Transport Packet layout

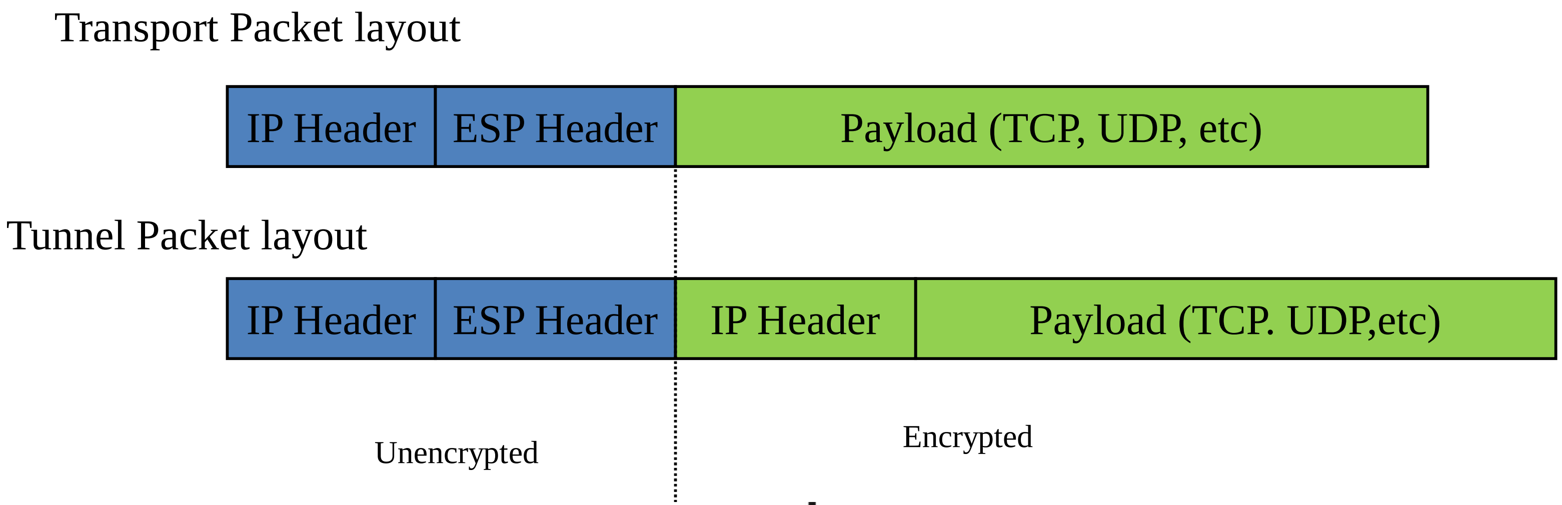
| | | |
|---|---|---|
| IP Header | AH Header | Payload (TCP, UDP, etc) |

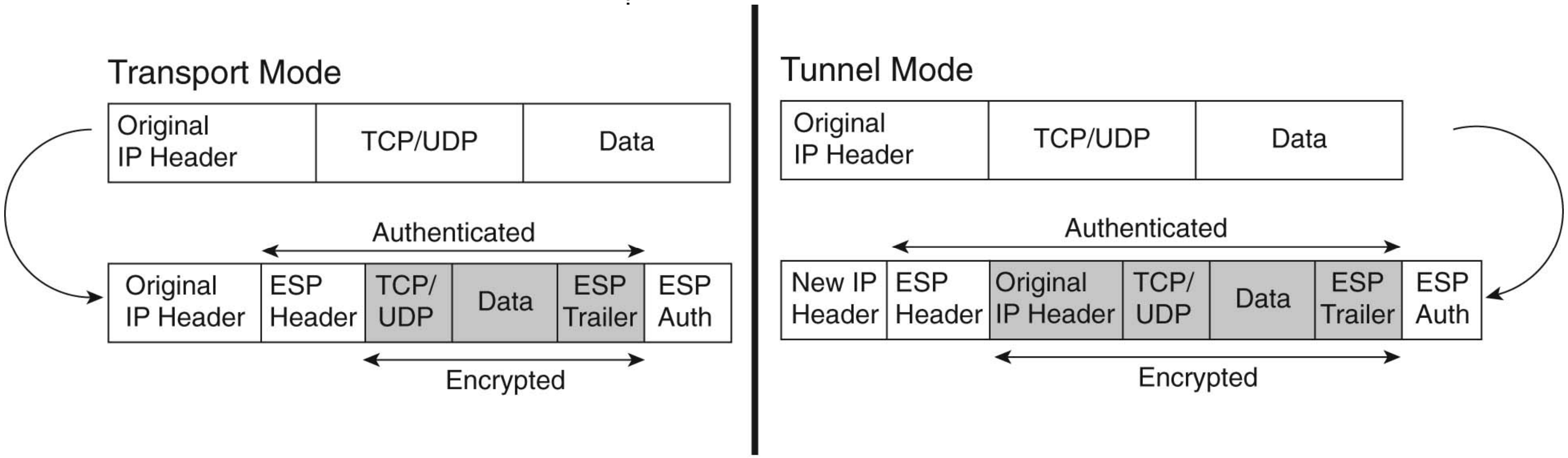
Tunnel Packet layout

| | | | |
|---|---|---|---|
| IP Header | AH Header | IP Header | Payload (TCP. UDP,etc) |



# IPSec Modes of Operation - ESP



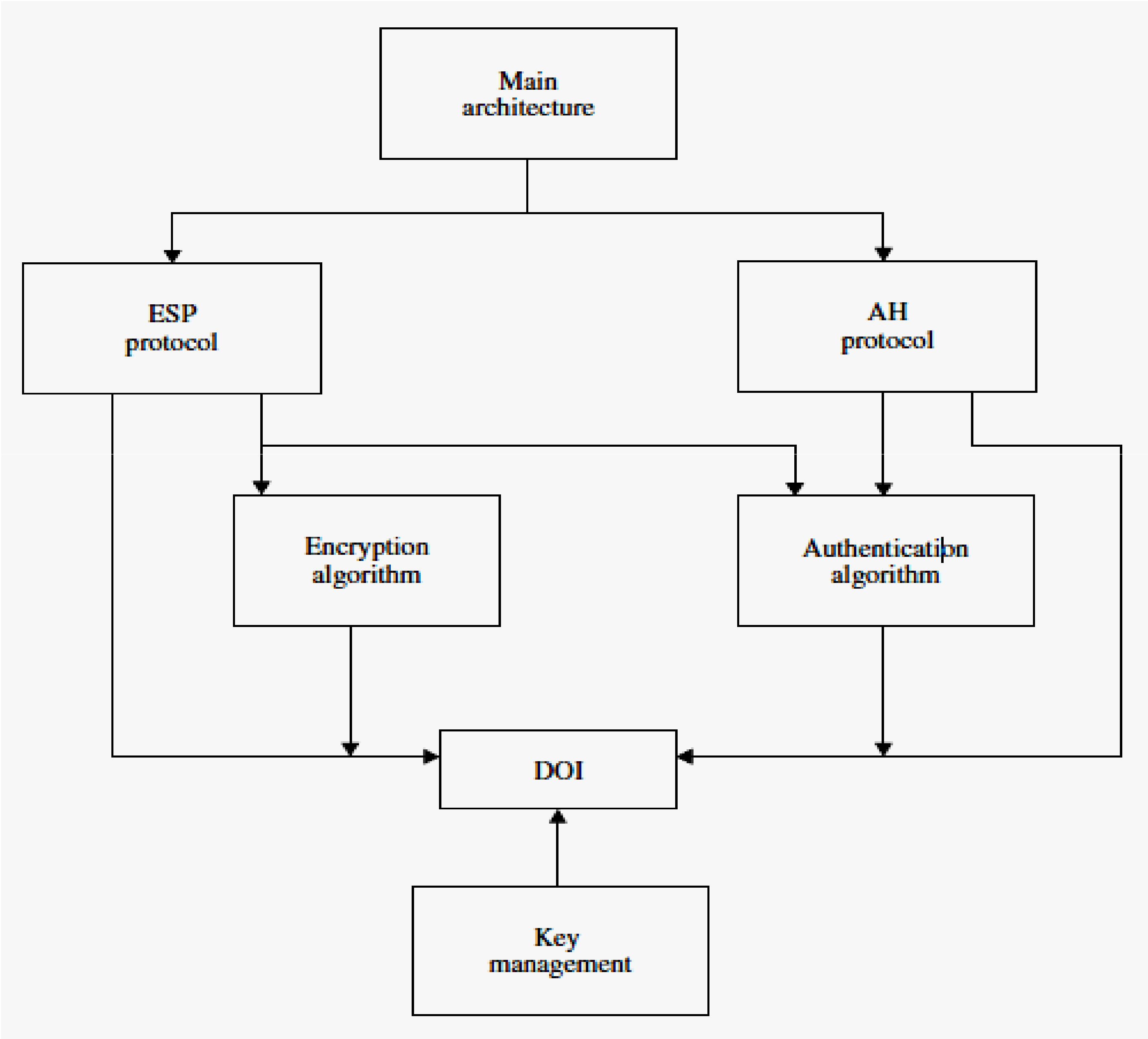
# IPSec Protocol

- Modular design
- Algorithm independent
  - Permits selection of different sets of algorithms without affecting the other parts of the implementation
  - Standard set of default algorithms is specified to facilitate interoperability in the global Internet
- Standard algorithms + IPSec traffic protection + key management protocols - deploy high-quality cryptographic security technology at Internet layer
- Provides high-quality security for Internet traffic

# IPSec Protocol Documents

- IP Security Document Roadmap - RFC 2411 by IETF - November 1998
- IPSec protocols is divided into seven groups
- Seven-group documents describes the set of IPSec protocols
    - *Architecture*
    - *ESP*
    - *AH*
    - *Encryption algorithm*
    - *Authentication algorithm*
    - *Key management*
    - *DOI :*Domain of Interpretation

# IPSec Protocol Documents / Architecture



# IPSec Protocol Documents

- Architecture:
  - Main document
  - Covers the general concepts, security requirements, definitions and mechanisms defining IPSec technology
- ESP:
  - Covers the packet format
  - General issues related to the use of the ESP for packet encryption and optional authentication
  - Contains default values
  - Dictates some of the values in the  Domain of Interpretation (DOI)
- AH:
  - Covers the packet format
  - General issue related to the use of AH for packet authentication
  - Contains default values such as the default padding contents
  - Dictates some of the values in the DOI document

# IPSec Protocol Documents

- Encryption algorithm:
  - Describe how various encryption algorithms are used for ESP
  - Specifically:
    - Specification of the key sizes and strengths for each algorithm
    - Any available estimates on performance of each algorithm
    - General information on how this encryption algorithm is to be used in ESP
    - Features of encryption algorithm
    - Provide input to the DOI
- Authentication algorithm:
  - Describe how various authentication algorithms are used for AH and for the authentication option of ESP
  - Specifically:
    - Specification of operating parameters such as number of rounds and input or output block format
    - Implicit and explicit padding requirements of this algorithm
    - Identification of optional parameters/methods of operation
    - Defaults and mandatory ranges of the algorithm
    - Comparison criteria for the algorithm
    - Method for verifying

# IPSec Protocol Documents

- Key management:
  - Describe key management schemes
  - Provide certain values for the DOI
  - Currently the key management represents the Oakley, ISAKMP
- DOI :
  - Contains values needed for the other documents to relate each other
  - These include identifiers for approved encryption and authentication algorithms
  - Operational parameters such as key lifetime

# Security Associations (SAs)

- RFC 1825
- Before sending data, a virtual connection is established from sending entity to receiving entity
- Called “security association (SA)”
  - SAs are simplex: for only one direction
  - One for inbound traffic
  - One for outbound traffic
  - A minimum of two SAs are required for a single IPSec connection
- Both sending and receiving entities maintain state information about the SA
- AH and ESP make use of SAs

# Security Associations (SAs)

- An SA is uniquely identified by three parameters
  1. Security Parameters Index (SPI)
  2. IP Destination Address
  3. Security Protocol Identifier

1. Security Parameters Index (SPI):
   - Assigned to each SA
   - Needed to identify an SA
   - Sender to communicate with a receiver, must know the SPI value for a particular SA
   - The SPI is carried in AH and ESP headers
   - Receiver identify a SA by the combination of SPI and destination address
   - SPI values are not globally specified

# Security Associations (SAs)

2. IP Destination Address:
    - Address of the destination endpoint of the SA
    - Destination endpoint may be an end-user system or a network system such as a firewall or router
    - Unicast addresses are only allowed by IPSec

3. Security Protocol Identifier:
    - This identifier indicates whether the association is an AH or ESP security association

# Security Associations (SAs)

- Two nominal databases
  - Security Policy Database (SPD)
  - Security Association Database (SAD)

    - Info in SPD indicates **“what”** to do with arriving datagram
      - specifies the policies that is to applied on all IP traffic

      ( inbound or outbound, from host or security gateways)
    - Info in the SAD indicates **“how”** to do it

# Security Policy Database (SPD)

- Essential element of SA processing
- Contains an ordered list of policy entries
- Specifies what services are to be offered to IP datagrams (use IPSec)
- Specifies what fashion (IPsec protocols, modes and algorithms to be employed)
- Policy decision on which SA to apply can be made on IP addresses (source or destination), protocol type or IP Header
- Used to control the flow of all traffic (inbound and outbound) through an IPsec system, including security and key management traffic (i.e. ISAKMP)

- Database specifies types of packets
  - to be dropped
  - to be forwarded or accepted under IPSec protection
  - to be forwarded or accepted without IPSec protection
  - to be encrypted or integrity protected

# Security Association Database (SAD)

- Endpoint holds state of its SAs in a SAD
- Helps in locating SA during processing
- While sending IPSec datagram, SAD is accessed to determine what SA to apply for process datagram
- When IPSec datagram arrives, the SPI in IPSec datagram is examined and indexes SAD with SPI, and processes datagram accordingly
- SA database at transmitter and receiver holds
    - cryptographic key
    - cryptographic algorithm
    - security services (e.g. encryption and/or integrity)
    - SPI
    - sequence number and ID of other end

- SPI (security Parameter Index) + destination address - uniquely identifies SA in database
- SPI of received packet tells where to look for info required to process packet

# Hashed Message Authentication Code (HMAC)

- HMAC is a secret-key authentication algorithm
- HMAC provides a data integrity check and data origin authentication for packets sent between two parties
- Generates Message Authentication Code (MAC)
- Based on a secret key - Shared between the client and server
- Keys are used for computation and verification of MAC
- Any iterative hash function can be used– HMAC, MD5, SHA-1, and RIPEMD-160
- Hash function module is replaced by any new , faster and secure hash function
- MD5 has been recently shown to be vulnerable to collision search attacks
- SHA-1 appears to be a cryptographically stronger function.

# Hashed Message Authentication Code (HMAC)

- Strength of HMAC depends
  - Strength of hash function
  - The size of its hash output
  - The size and quality of the key

# *HMAC Structure*

Requires

- H - Cryptographic hash function
  - Iterating compression function on data blocks
- K - Secret key - any length up to b = 512 bits
- b - Block length
- H - Length of hash values
  - 16 bytes or 128 bits for MD5
  - 20 bytes or 160 bits for SHA-1
- M – is the message to be authenticated

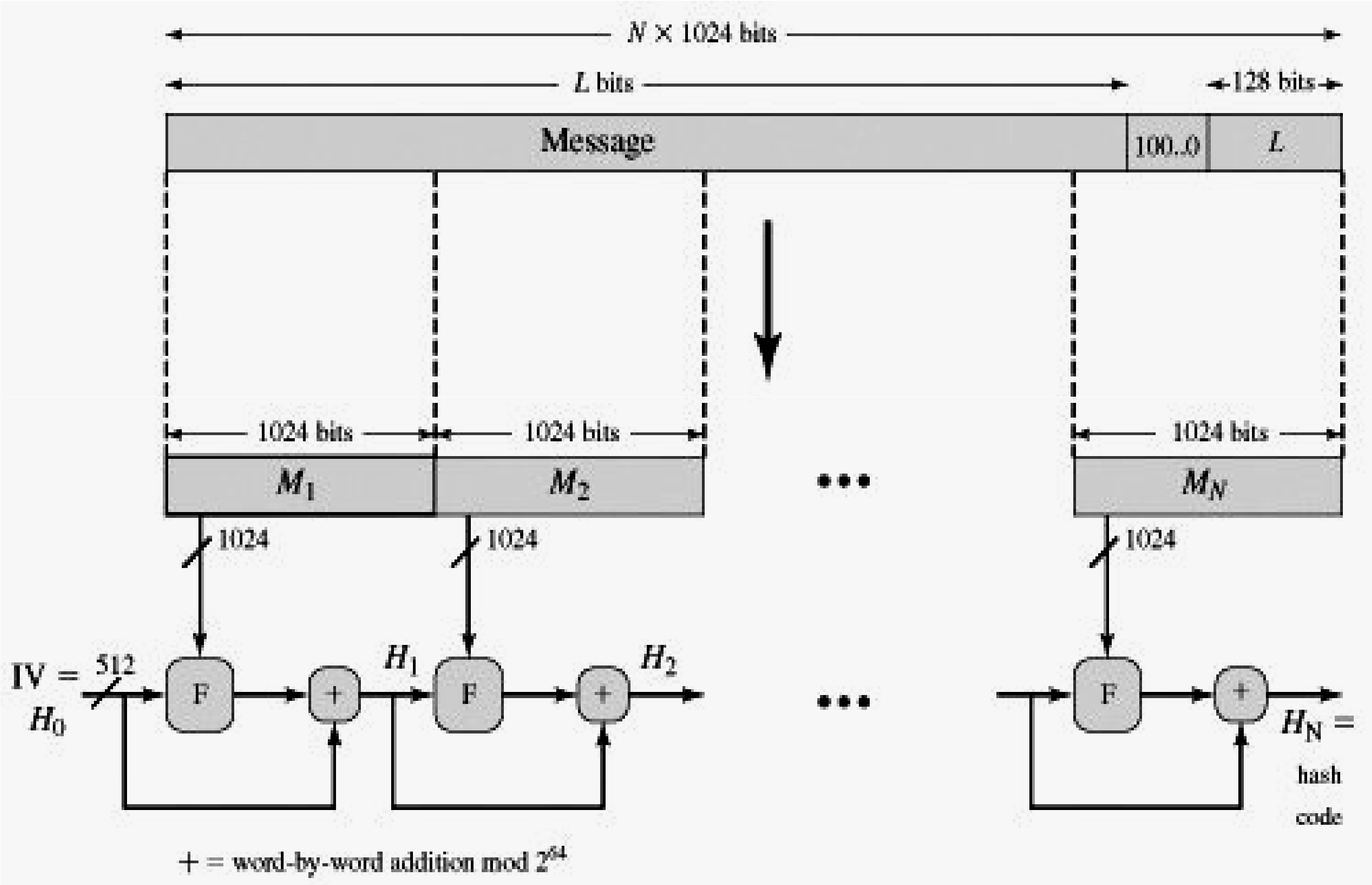
# *HMAC Structure*

To compute HMAC over the message, the HMAC equation is expressed as follows:

$$HMAC = H[\ (K \oplus opad)\ ||\ H[\ (K \oplus ipad)||M]\ ]$$

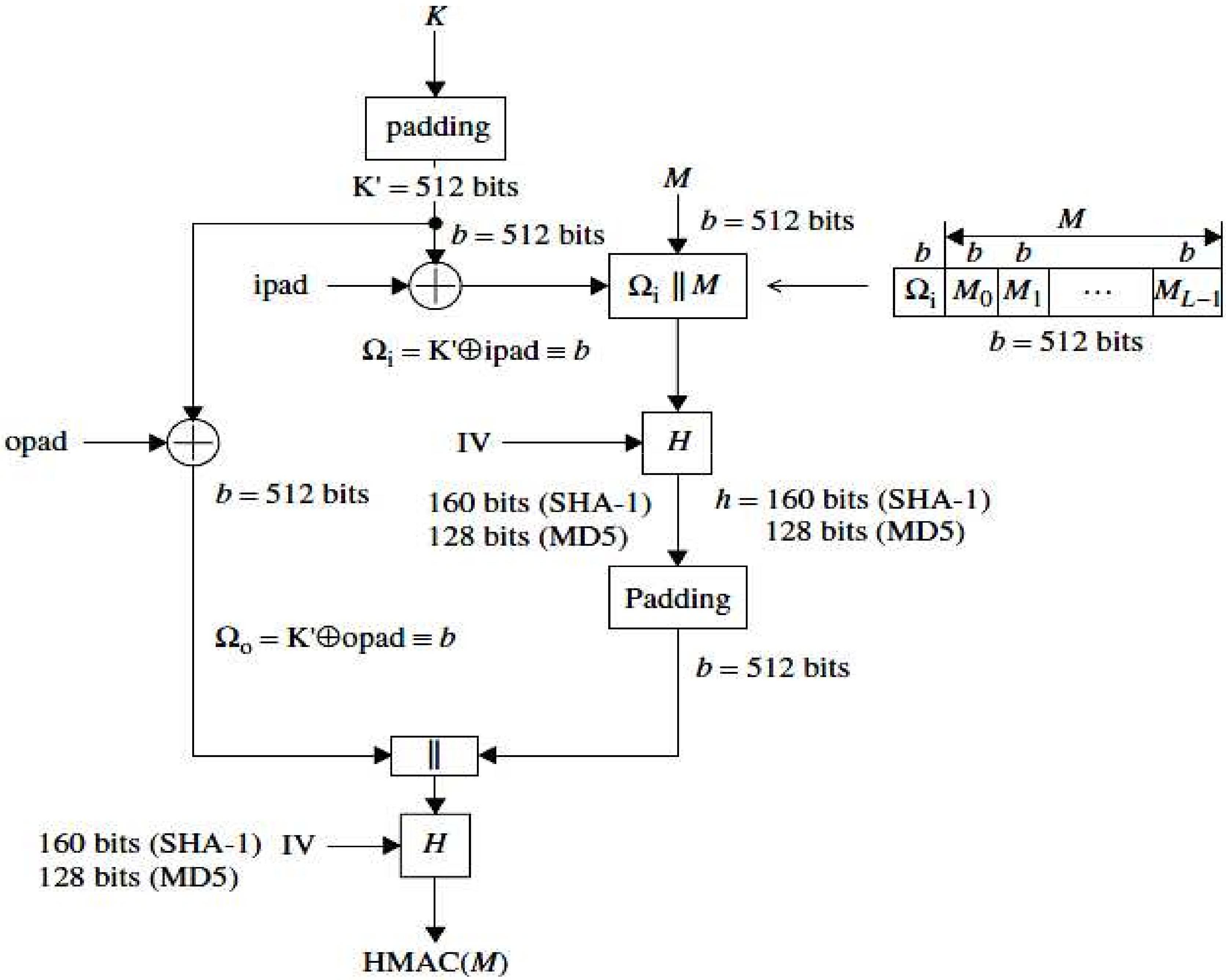
- where
  - ipad = 00110110*(0x36) repeated 64 times (512 bits)*
  - opad = 01011100*(0x5c) repeated 64 times (512 bits)*
  - ipad is inner padding
  - opad is outer padding

# HMAC



N × 1024 bits
L bits
128 bits
Message
100..0
L
1024 bits
1024 bits
1024 bits
M1
M2
MN
1024
1024
1024
IV =
H0
512
F
+
H1
F
+
H2
F
+
HN =
hash
code
+ = word-by-word addition mod 2^64

# *HMAC Structure*



# *HMAC Structure*

The following explains the HMAC equation:

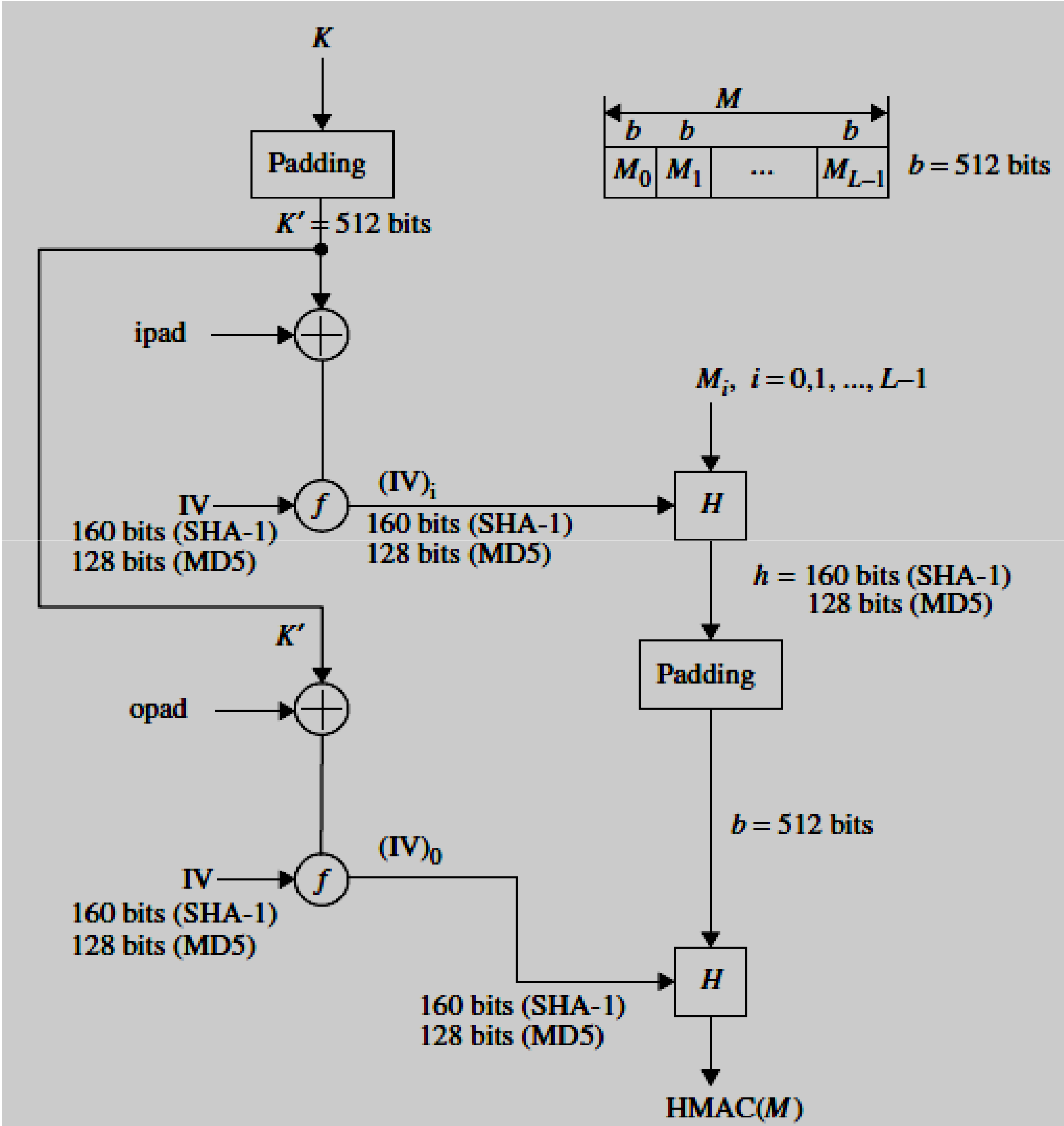
1. Append zeros to the end of *K to create a b-byte string* *(i.e. if K = 160 bits in length* and *b = 512 bits, then K will be appended with 352 zero bits or 44 zero bytes 0x00)*
2. XOR (bitwise exclusive-OR) *K with ipad to produce the b-bit block computed in* step 1
3. Append *M to the b-byte string resulting from step 2 .*
4. Apply *H to the stream generated in step 3*
5. XOR (bitwise exclusive-OR) *K with opad to produce the b-byte string computed in* step 1
6. Append the hash result *H from step 4 to the b-byte string resulting from step 5*
7. Apply *H to the stream generated in step 6 and output the result*

# *HMAC Structure*

Alternative

1. Append zeros to *K to create a b-bit string K* , where *b = 512 bits*
2. XOR *K* (padding with zero) with ipad to produce the *b-bit block*
3. Apply the compression function f(IV, *K* ⊕ ipad) to produce (IV)i = 128 bits
4. Compute the hash code *h with (IV)i and Mi*
5. Raise the hash value computed from step 4 to a *b-bit string*
6. XOR *K* (padded with zeros) with opad to produce the *b-bit block*
7. Apply the compression function f(IV, *K'⊕opad) to produce (IV)0 = 128 bits*
8. Compute the HMAC with (IV)o and the raised hash value resulting from step 5. operation

# Alternative HMAC



# Summary

- IPSec Protocol Documents
    - *Architecture*
    - *ESP*
    - *AH*
    - *Encryption algorithm*
    - *Authentication algorithm*
    - *Key management*
    - *DOI :*Domain of Interpretation
- Security Associations (SAs)
    - Security Policy Database (SPD)
    - Security Association Database (SAD)
- Hashed Message Authentication Code (HMAC)
    - HMAC = H[ (K $\oplus$ opad) || H[ (K $\oplus$ ipad)||M] ]