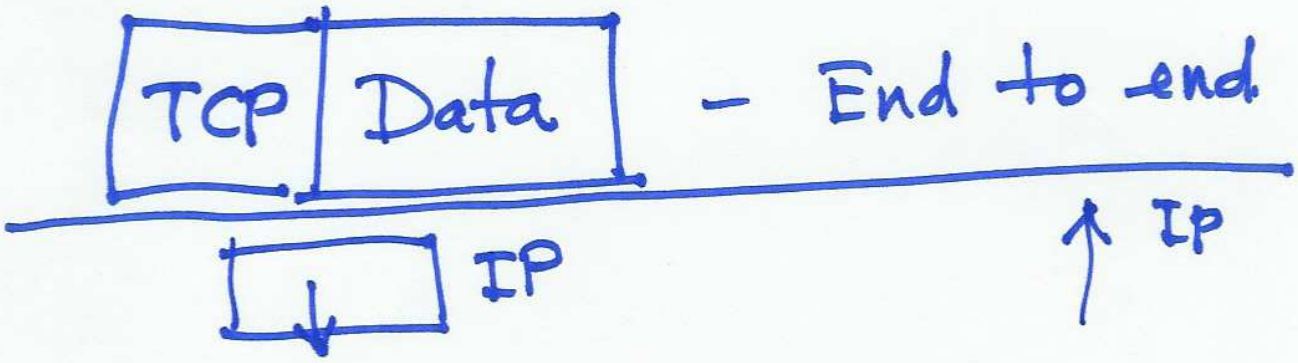
# 4/12/07

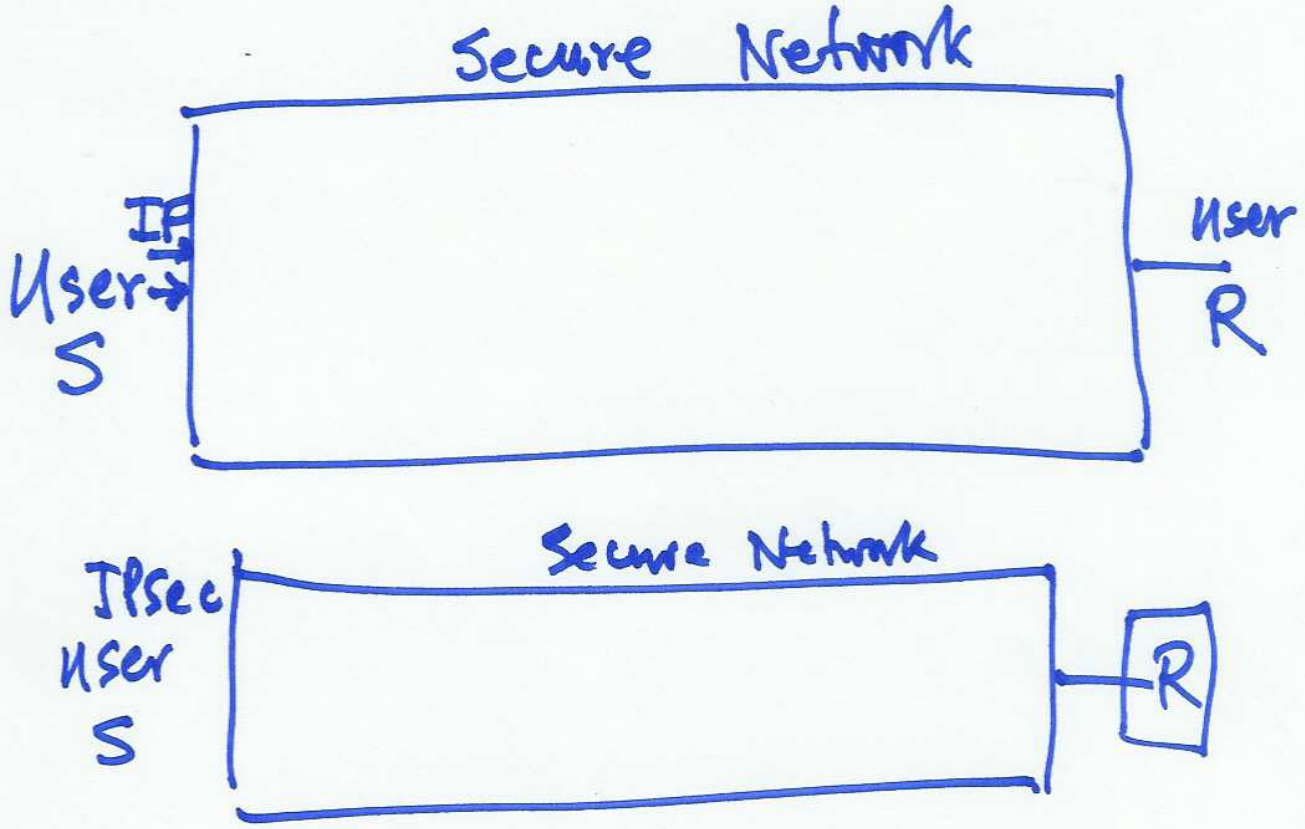
# IPsec




S Connectionless R

IPsec - Provide security in the network.

Solution for Network Security







IPsec

(1) Authentication

(2) Confidentiality

(3) Key Management

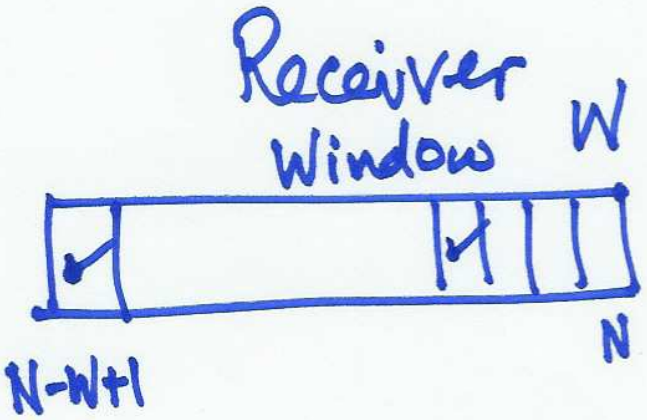
# 1) Authentication Header AH

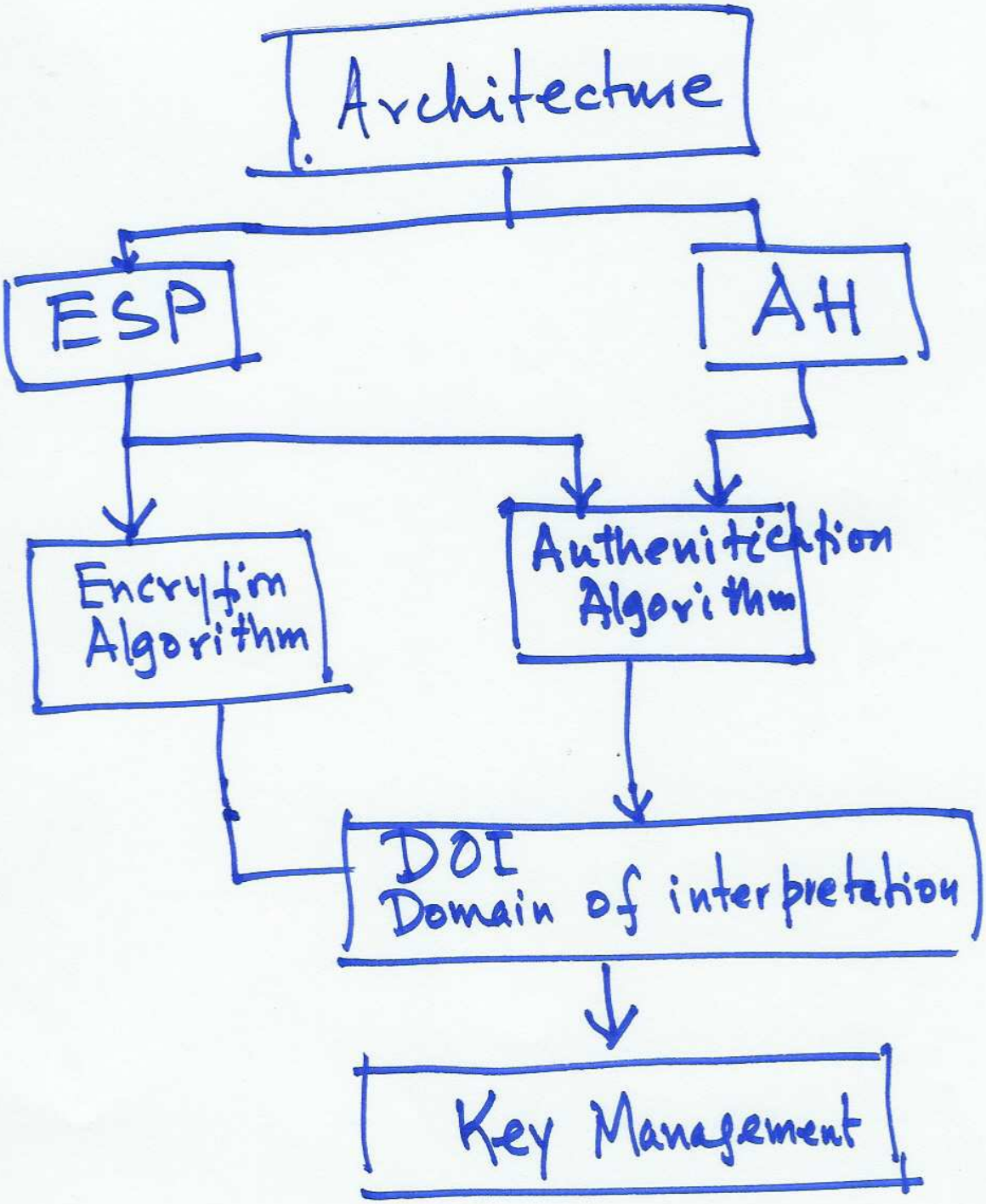
# (2) ESP - Encapsulating Security Payload.

| AH | ESP (Encrypt) | ESP (Encrypt + Authentication) |
|---|---|---|
| Access Control | ~~Yes~~ | Yes |
| Comm Integrity | | Yes |
| Data origination authentication | | Yes |
| Replayed attack determined | Yes | Yes |
| | Confidentiality | Yes |
| | Limited traffic flow Confidentiality | Yes |

# Replayed attack

32 bit
sequence no.




Architecture
ESP
AH
Encryption Algorithm
Authentication Algorithm
DOI
Domain of interpretation
Key Management

Database

Security Association Database

(SA)

Transmit IPsec to destination X

S - how to transmit,
Security parameters Index
Key, the algorithm, seq no.

Security Policy Database

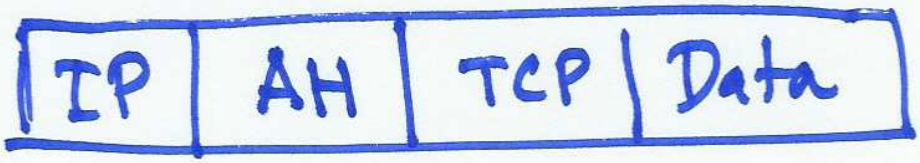
# AH.

## IPv4 and IPv6

(1) Transport Mode
(2) Tunnel Mode.



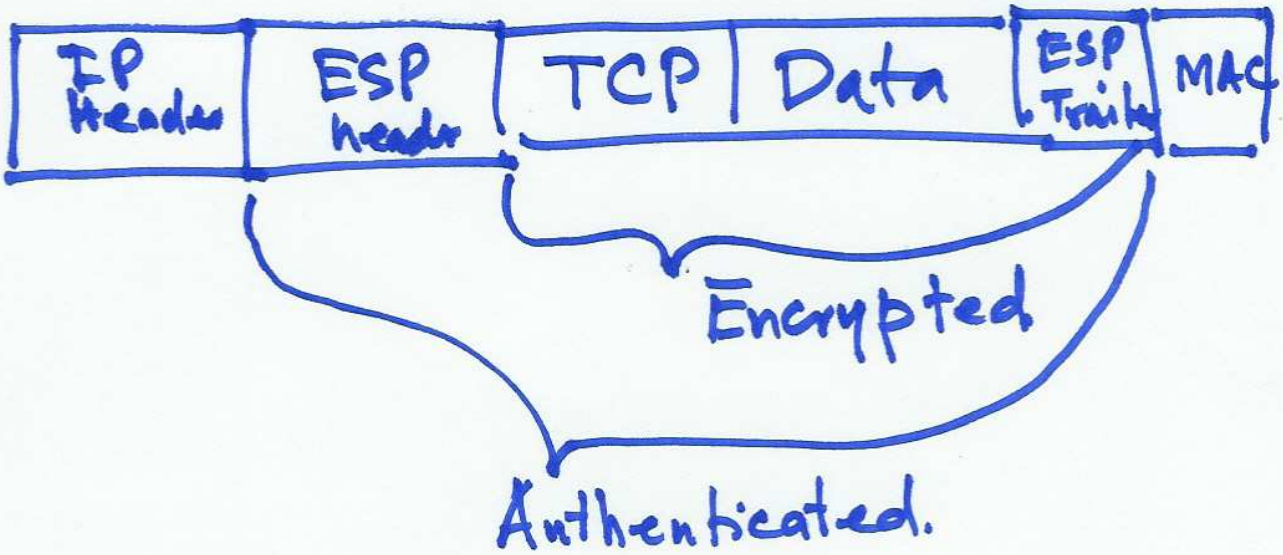
AH




AH - Next Header
Payload length - AH in terms of 32 bit word
SPI
Sequence no.
MAC, ICV

# Tunnel Mode


# ESP Transport Mode




HMAC - MD5 } - 96 bits
SHA-1 }