

Fall 2008: CS442  
Intro. to Computer Security

Vinod Ganapathy  
Lecture 19

Material from Chapter 21.

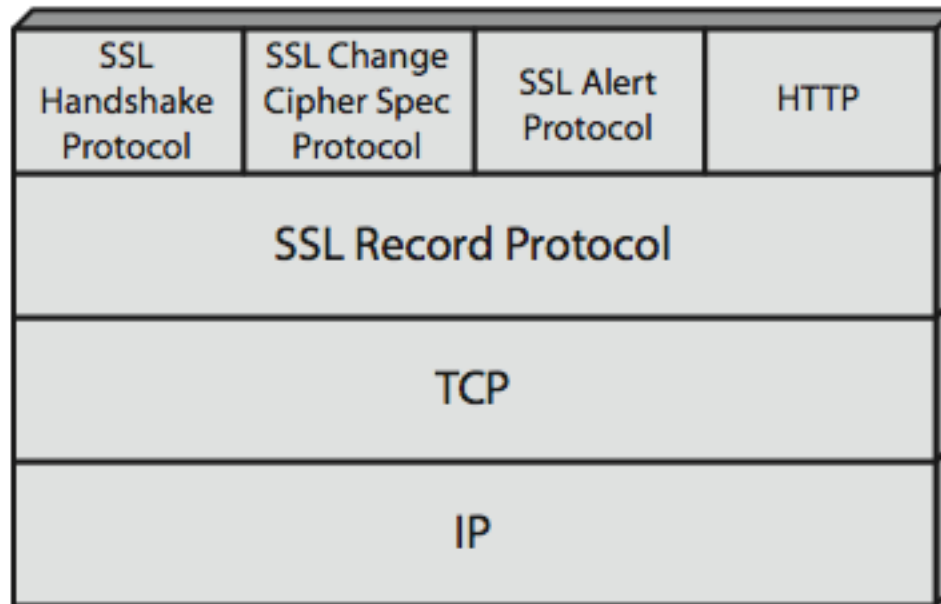
# Internet Security Protocols and Standards

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- IPv4 and IPv6 Security
- S/MIME (Secure/Multipurpose Internet Mail Extension)

# Secure Sockets Layer (SSL)

- transport layer security service
  - originally developed by Netscape
  - version 3 designed with public input
- subsequently became Internet standard  
RFC2246: Transport Layer Security (TLS)
- use TCP to provide a reliable end-to-end service
- may be provided in underlying protocol suite
- or embedded in specific packages

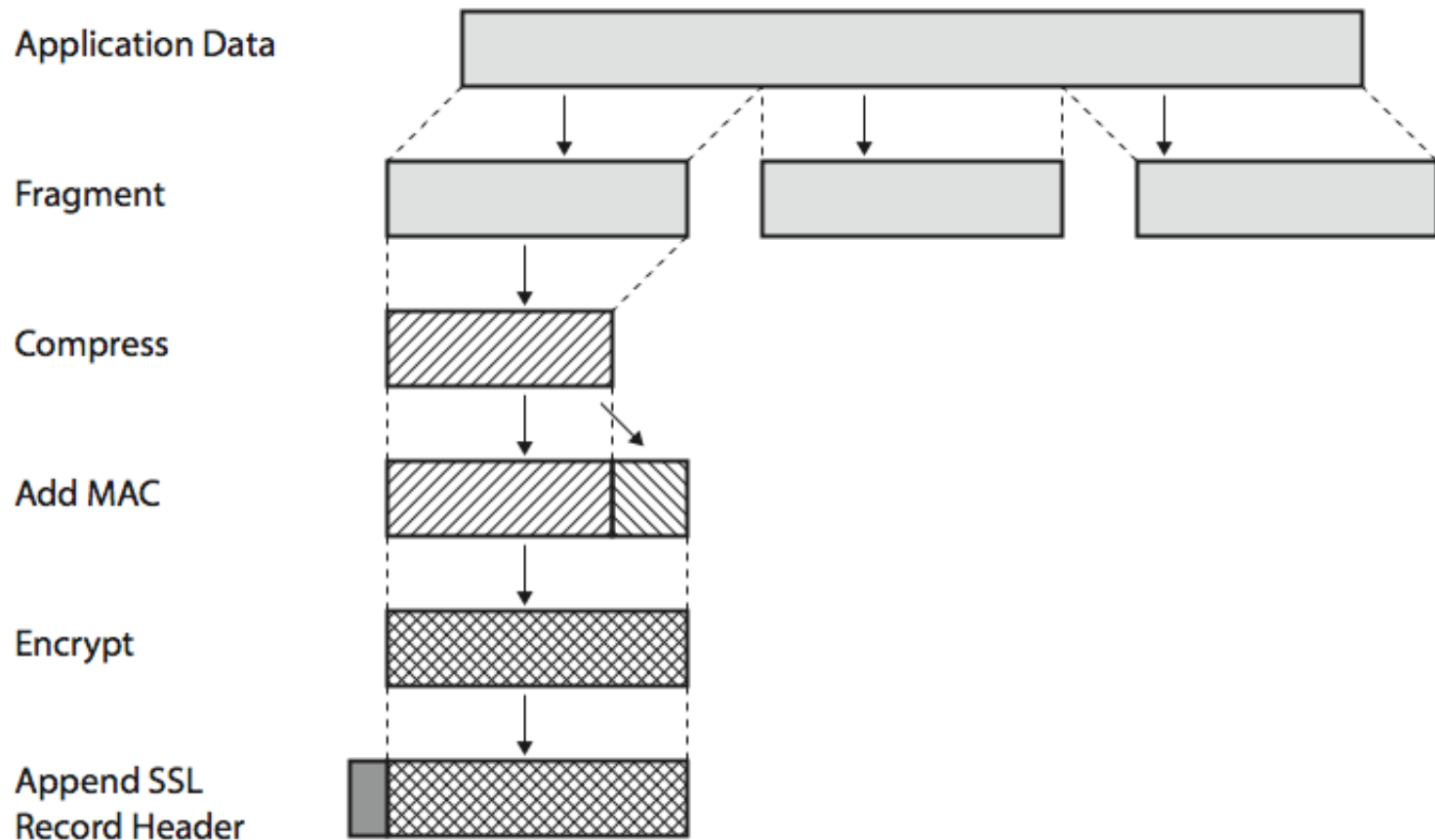
# SSL Protocol Stack



# SSL Record Protocol Services

- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding
- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - message is compressed before encryption

# SSL Record Protocol Operation



# SSL Change Cipher Spec Protocol

- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use

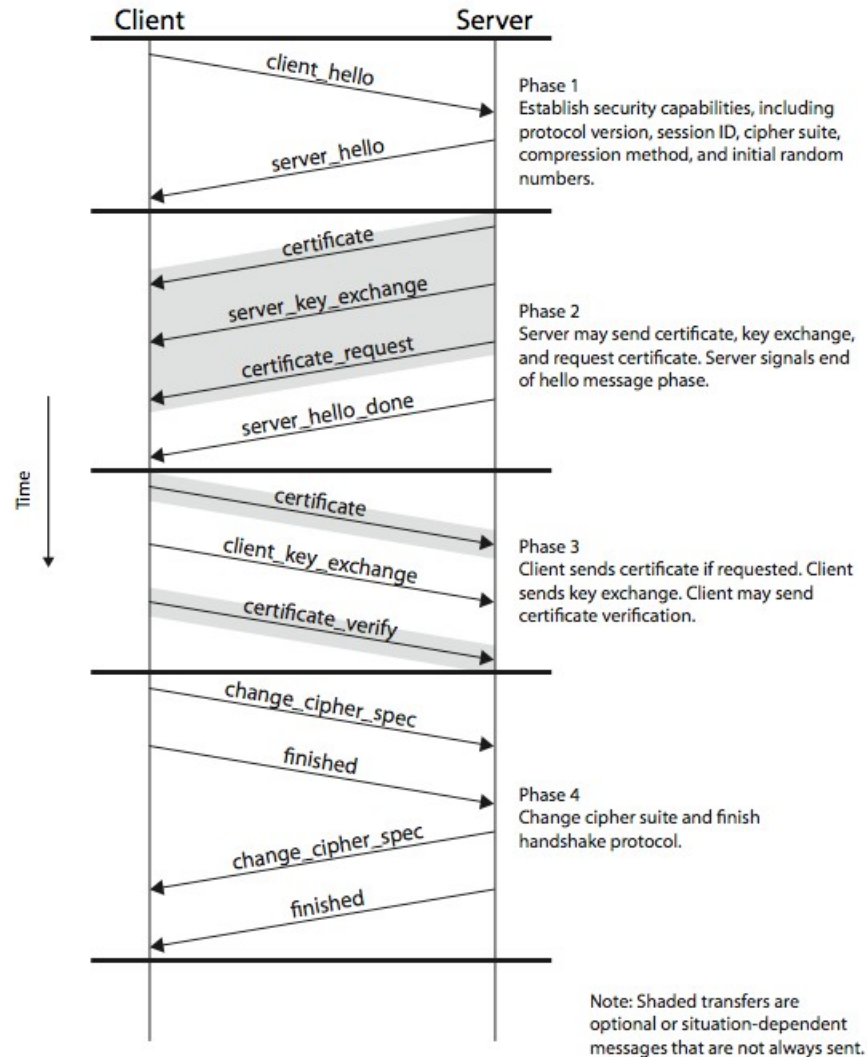
# SSL Alert Protocol

- conveys SSL-related alerts to peer entity
- severity
  - warning or fatal
- specific alert
  - fatal: unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

# SSL Handshake Protocol

- allows server & client to:
  - authenticate each other
  - to negotiate encryption & MAC algorithms
  - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  1. Establish Security Capabilities
  2. Server Authentication and Key Exchange
  3. Client Authentication and Key Exchange
  4. Finish

# SSL Handshake Protocol



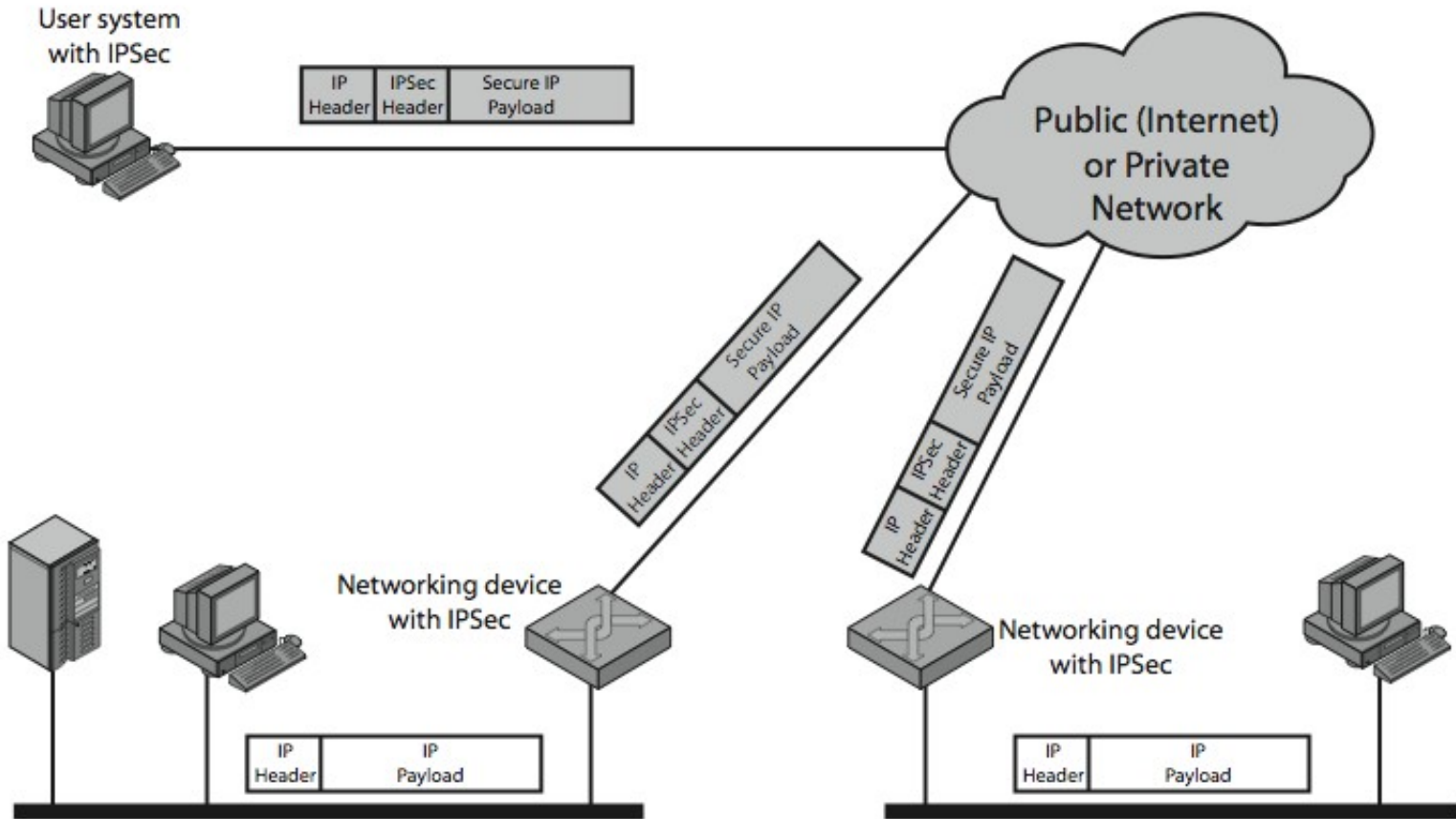
# IP Security

- various application security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- security concerns cross protocol layers
- hence would like security implemented by the network for all applications
- authentication & encryption security features included in next-generation IPv6
- also usable in existing IPv4

# IPSec

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

# IPSec Uses



# Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

# IP Security Architecture

- mandatory in IPv6, optional in IPv4
- have two security header extensions:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Key Exchange function
- VPNs want both authentication/encryption
  - hence usually use ESP
- specification is quite complex
  - numerous RFC's 2401/2402/2406/2408

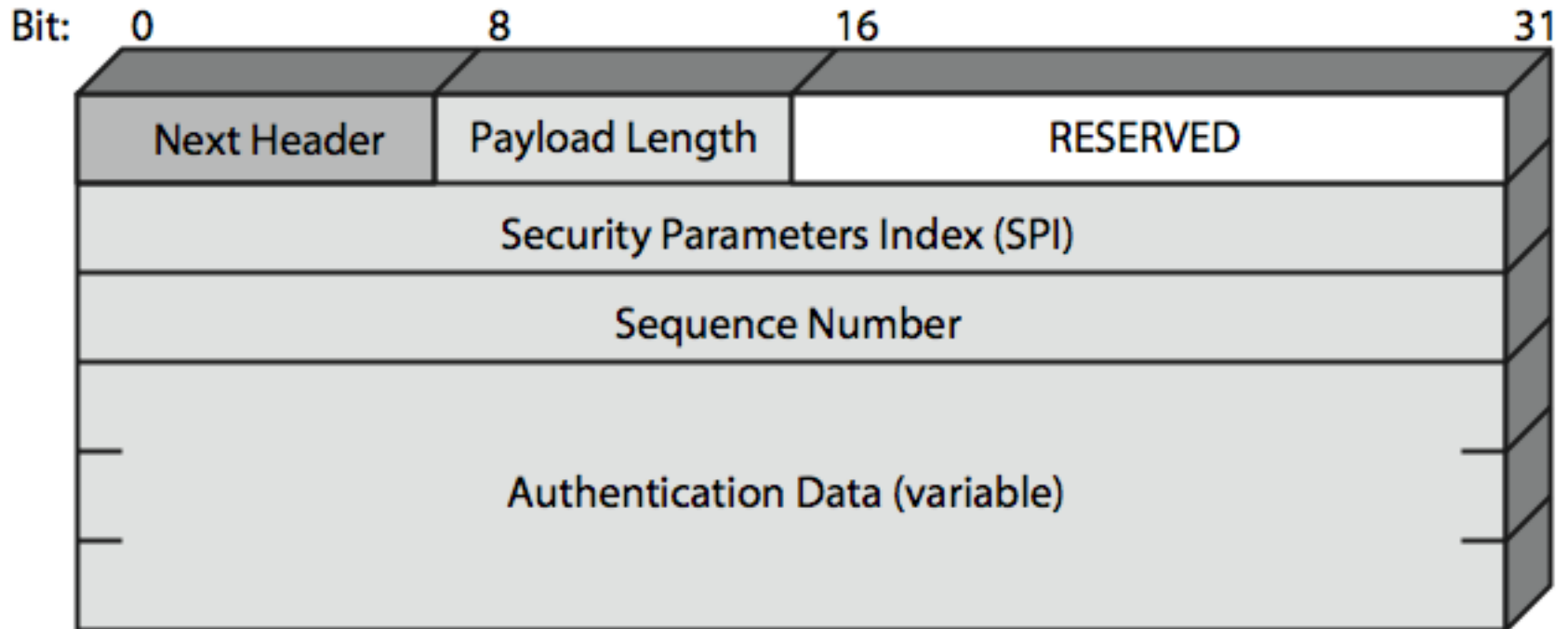
# Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

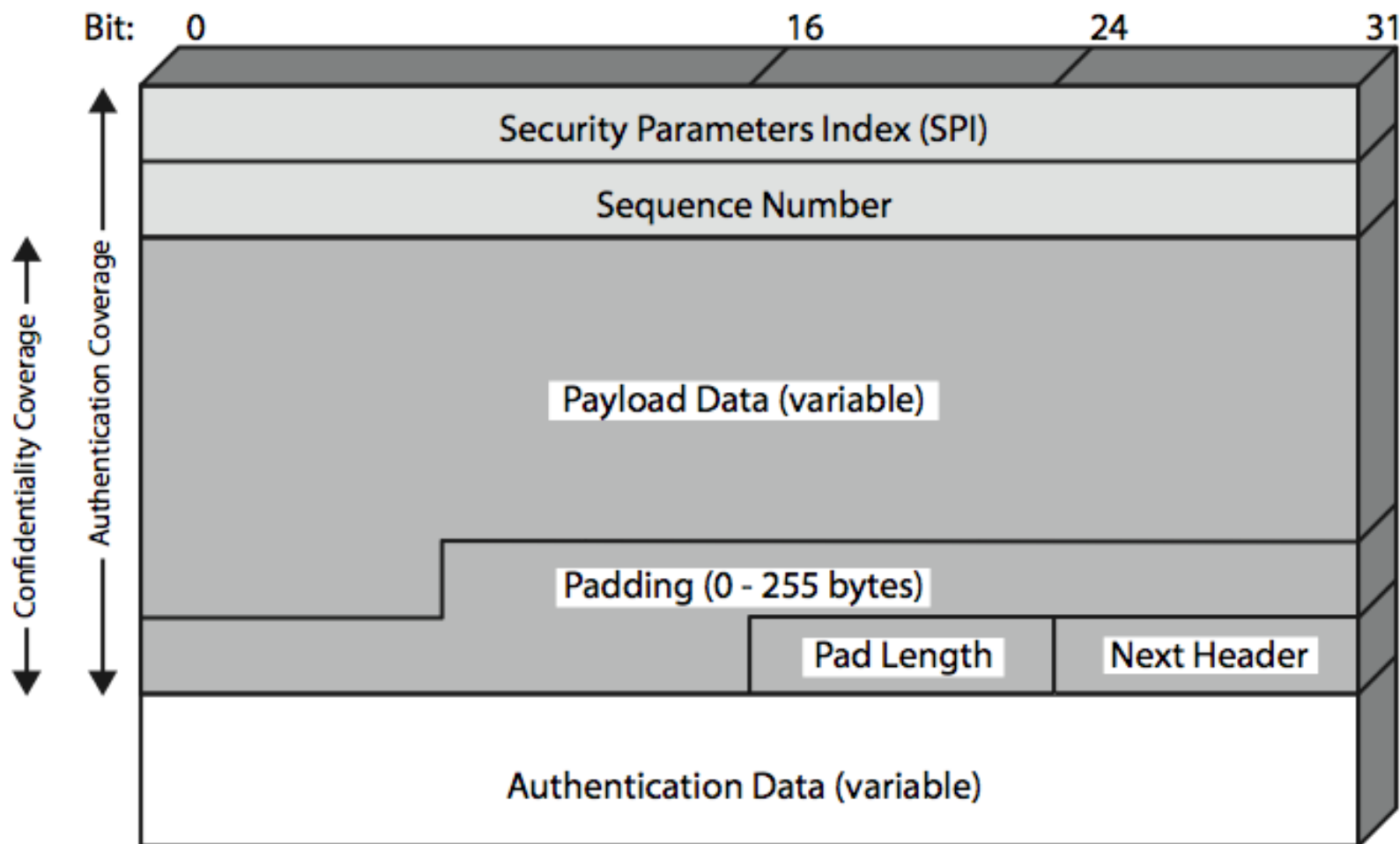
# Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

# Authentication Header



# Encapsulating Security Payload (ESP)



# Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

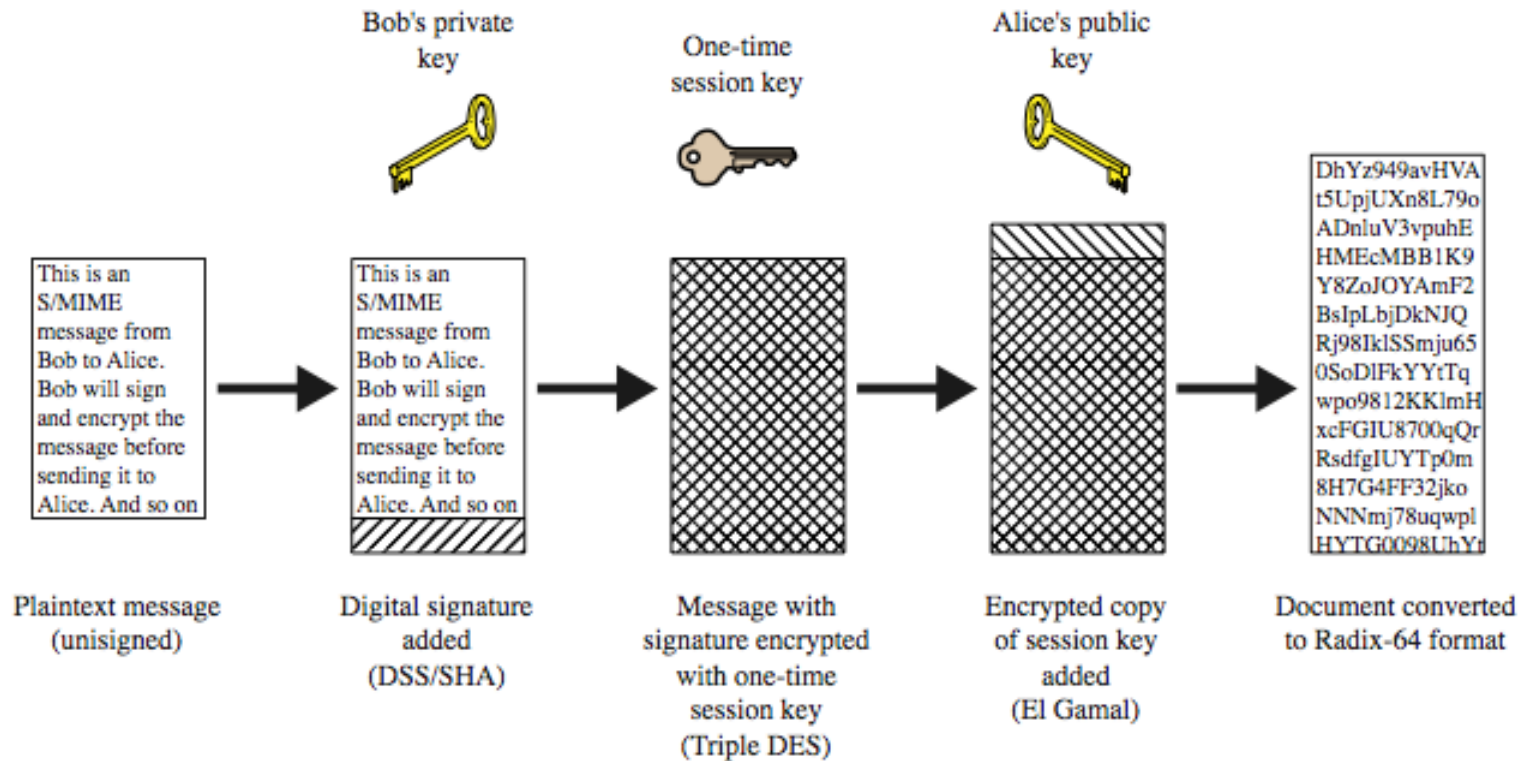
# S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
  - original Internet RFC822 email was text only
  - MIME provided support for varying content types and multi-part messages
  - with encoding of binary data to textual form
  - S/MIME added security enhancements
- have S/MIME support in many mail agents
  - eg MS Outlook, Mozilla, Mac Mail etc

# S/MIME Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

# S/MIME Process



# S/MIME Cryptographic Algorithms

- digital signatures: DSS & RSA
- hash functions: SHA-1 & MD5
- session key encryption: ElGamal & RSA
- message encryption: AES, 3DES, etc
- MAC: HMAC with SHA-1
- must map binary values to printable ASCII
  - use radix-64 or base64 mapping

# S/MIME Public Key Certificates

- S/MIME has effective encryption and signature services
- but also need to manage public-keys
- S/MIME uses X.509 v3 certificates
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's

# Summary

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- IPv4 and IPv6 Security
- S/MIME (Secure/Multipurpose Internet Mail Extension)