Network Security Part II: Standards

Raj Jain
Washington University
Saint Louis, MO 63131
Jain@cse.wustl.edu

These slides are available on-line at:

http://www.cse.wustl.edu/~jain/cse473-05/

- Secret Key Encryption:
  - Data encryption standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (**AES**)
- Hashing:
  - Secure Hash Algorithm 1 (**SHA1**)
- Secure Socket Layer (**SSL**)
- Secure IP (**IPSec**)

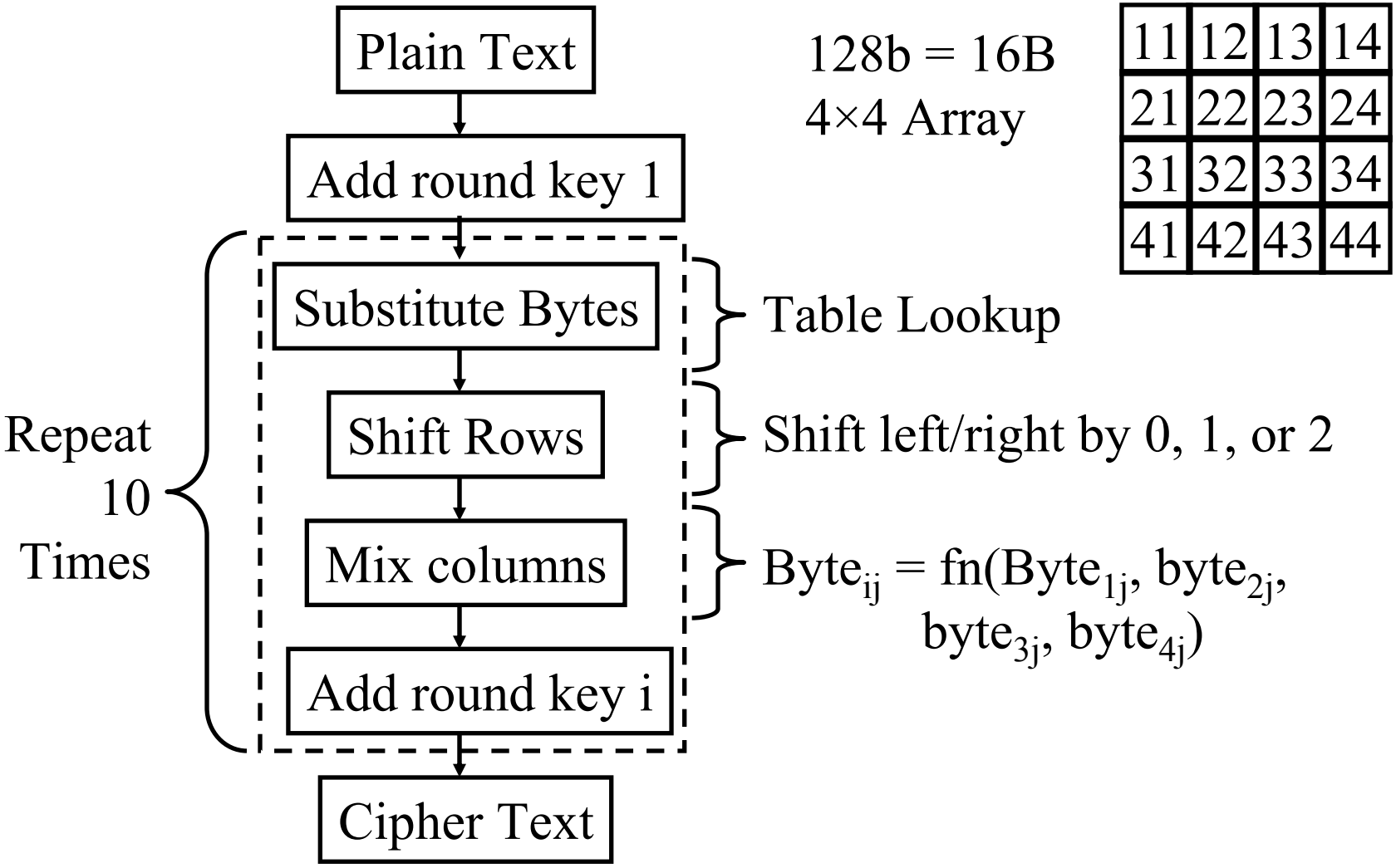
DES and 3DES

- Data Encryption Standard (DES)
  - 64 bit plain text blocks, 56 bit key
  - Broken in 1998 by Electronic Frontier Foundation
- Triple DES (3DES)
  - Uses 2 or 3 keys and 3 executions of DES
  - Effective key length 112 or 168 bit
  - Block size (64 bit) too small $\Rightarrow$ Slow

Advanced Encryption Standard (AES)

- Designed in 1997-2001 by National Institute of Standards and Technology (NIST)
- Federal information processing standard (FIPS 197)
- Symmetric block cipher, Block length 128 bits
- Key lengths 128, 192, and 256 bits

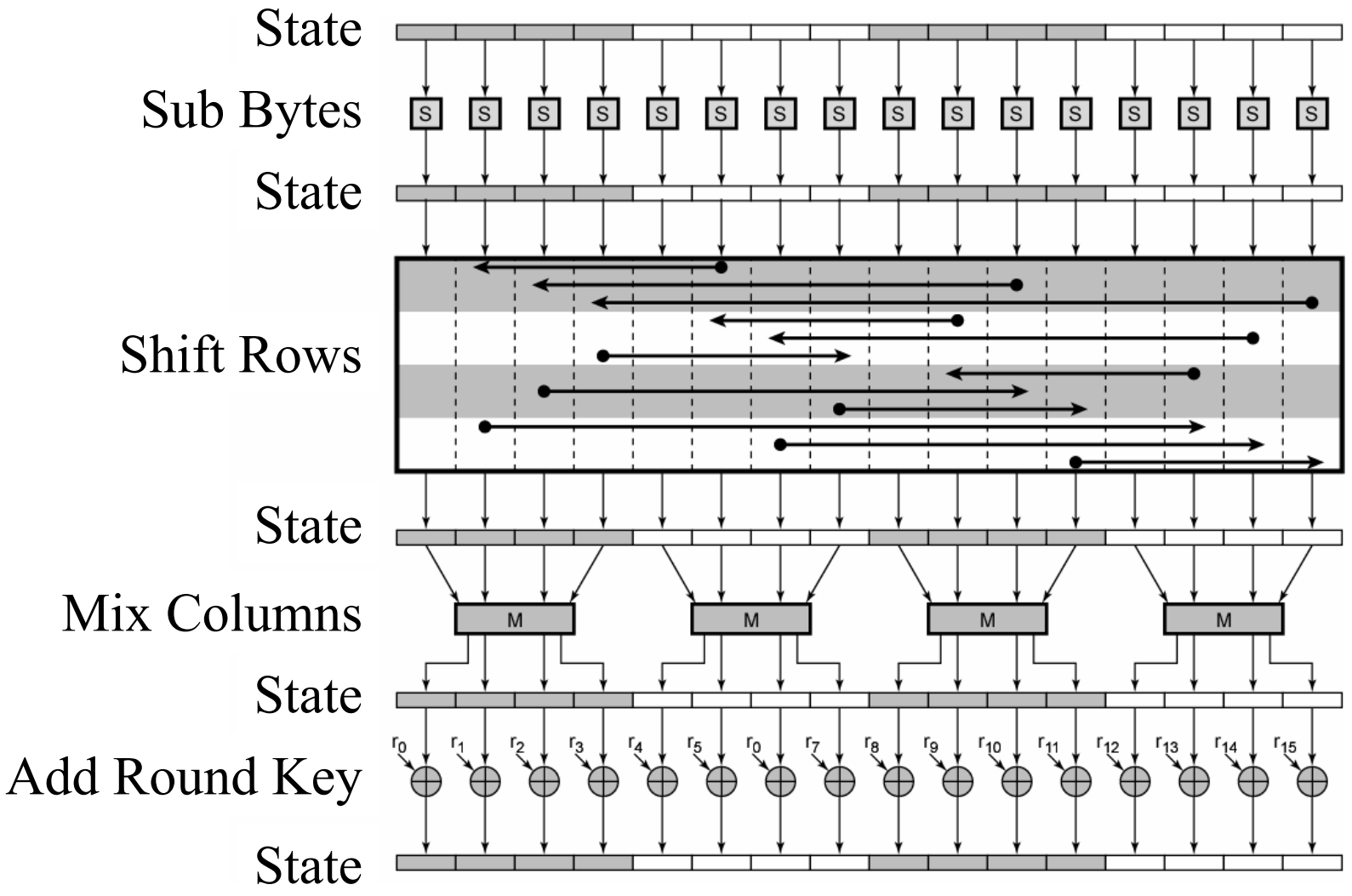
AES (cont)



128b = 16B
4×4 Array

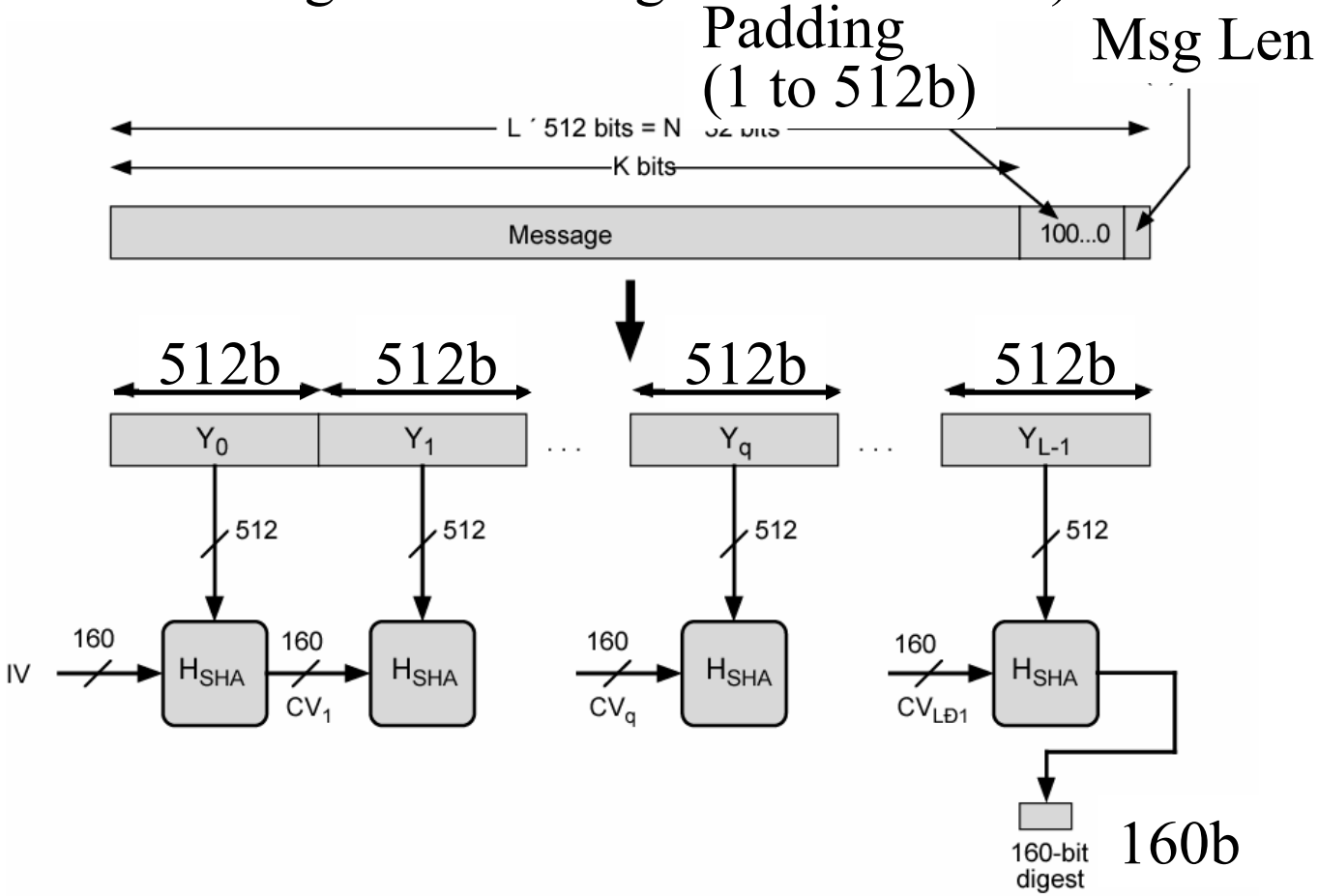
11	12	13	14
21	22	23	24
31	32	33	34
41	42	43	44

AES Encryption Round



Secure Hash Algorithm 1 (SHA-1)

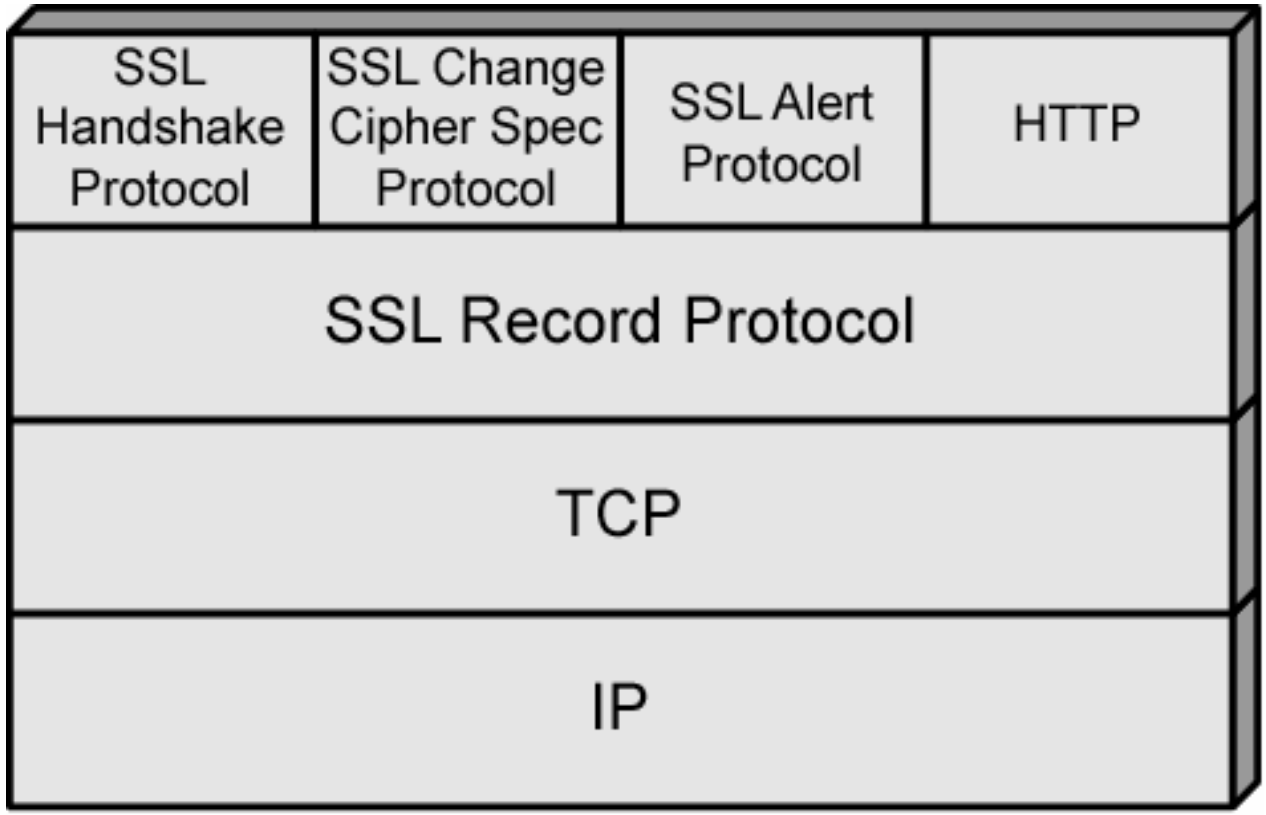
- Data processed in 512 bit blocks ⇒ 160 bit hash
- 1-512 bit Padding + 64 bit length (Data < 2^{64} b)



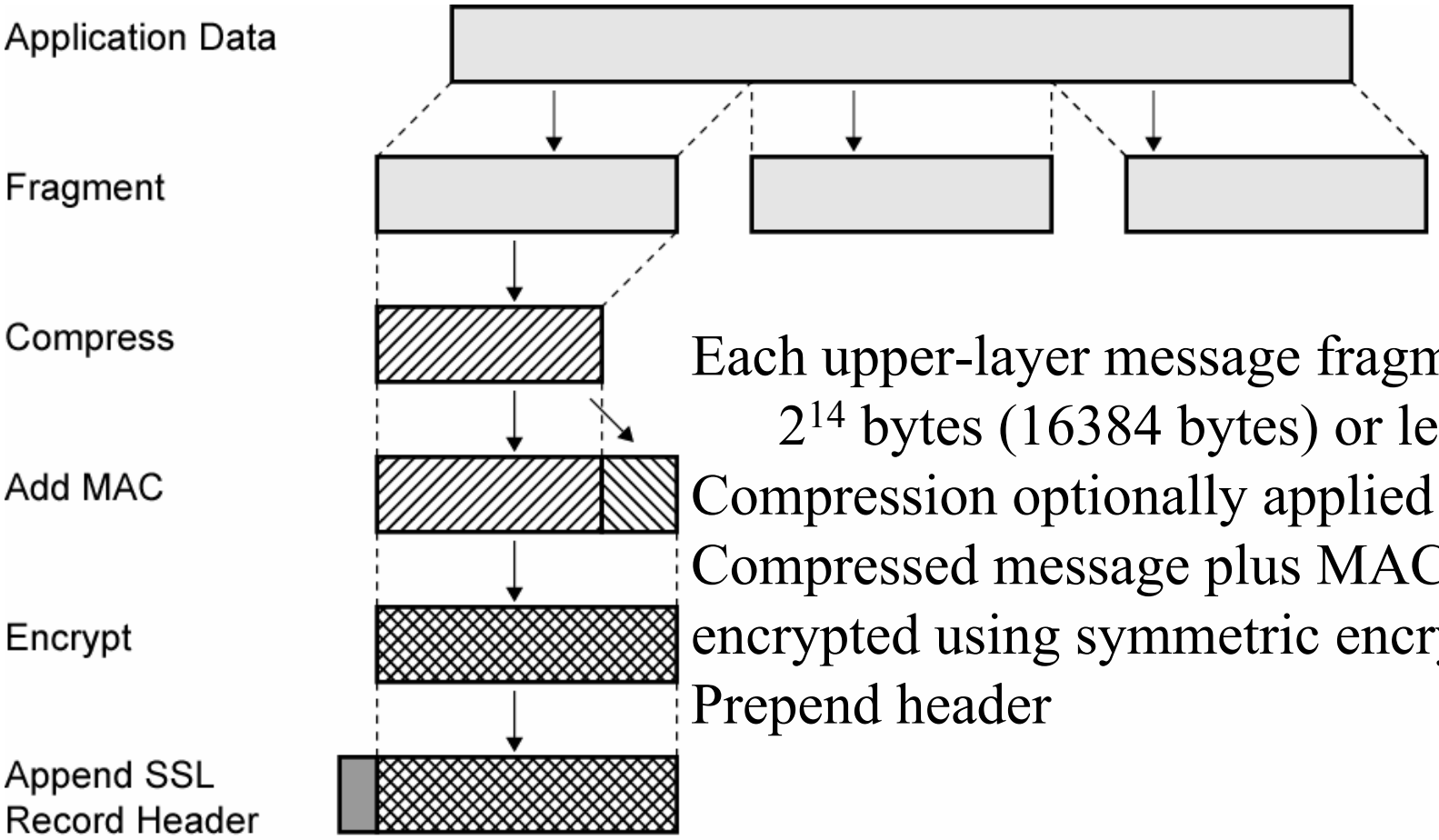
SSL and TLS

- Secure Socket Layer (SSL)
  Reliable end-to-end secure service over TCP
- Embedded in specific packages, E.g., Netscape and Microsoft Explorer and most Web servers
- Transport Layer Security (TLS) defined in RFC 2246
- Minor differences between SSLv3 and TLS
- Session = Multiple end-to-end TCP connections
- Four Protocols:
  - Handshake protocol: Exchange shared secret key
  - Record protocol: Provide end-to-end encryption
  - Change cipher spec protocol: Updates cipher suite
  - Alert protocol: Warnings and fatal errors to peer

SSL Protocol Stack

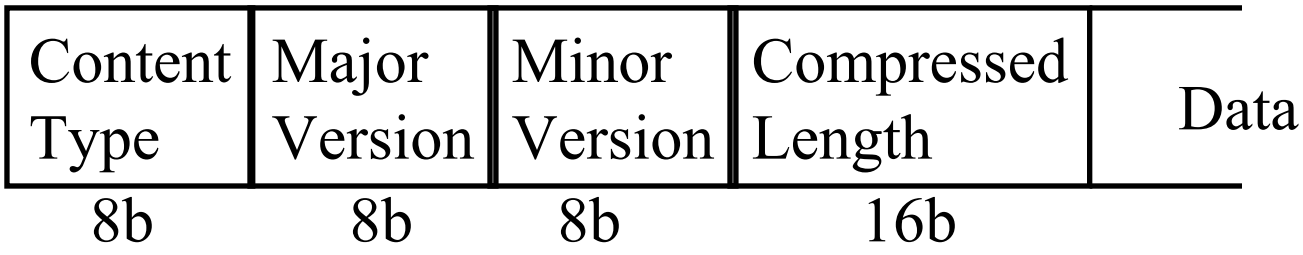


SSL Record Protocol Operation



Each upper-layer message fragmented
2^{14} bytes (16384 bytes) or less
Compression optionally applied
Compressed message plus MAC
encrypted using symmetric encryption
Prepend header

Record Protocol Header



- Content Type: change_cipher_spec, alert, handshake, and application_data
- Major Version: SSL v3 is 3
- Minor Version: SSLv3 value is 0
- Compressed Length: Maximum $2^{14} + 2048$

Change Cipher Spec Protocol

- Cause pending state to be copied into current state
  - Updates cipher suite to be used on this connection
- Single message: Single byte value 1
- Uses Record Protocol

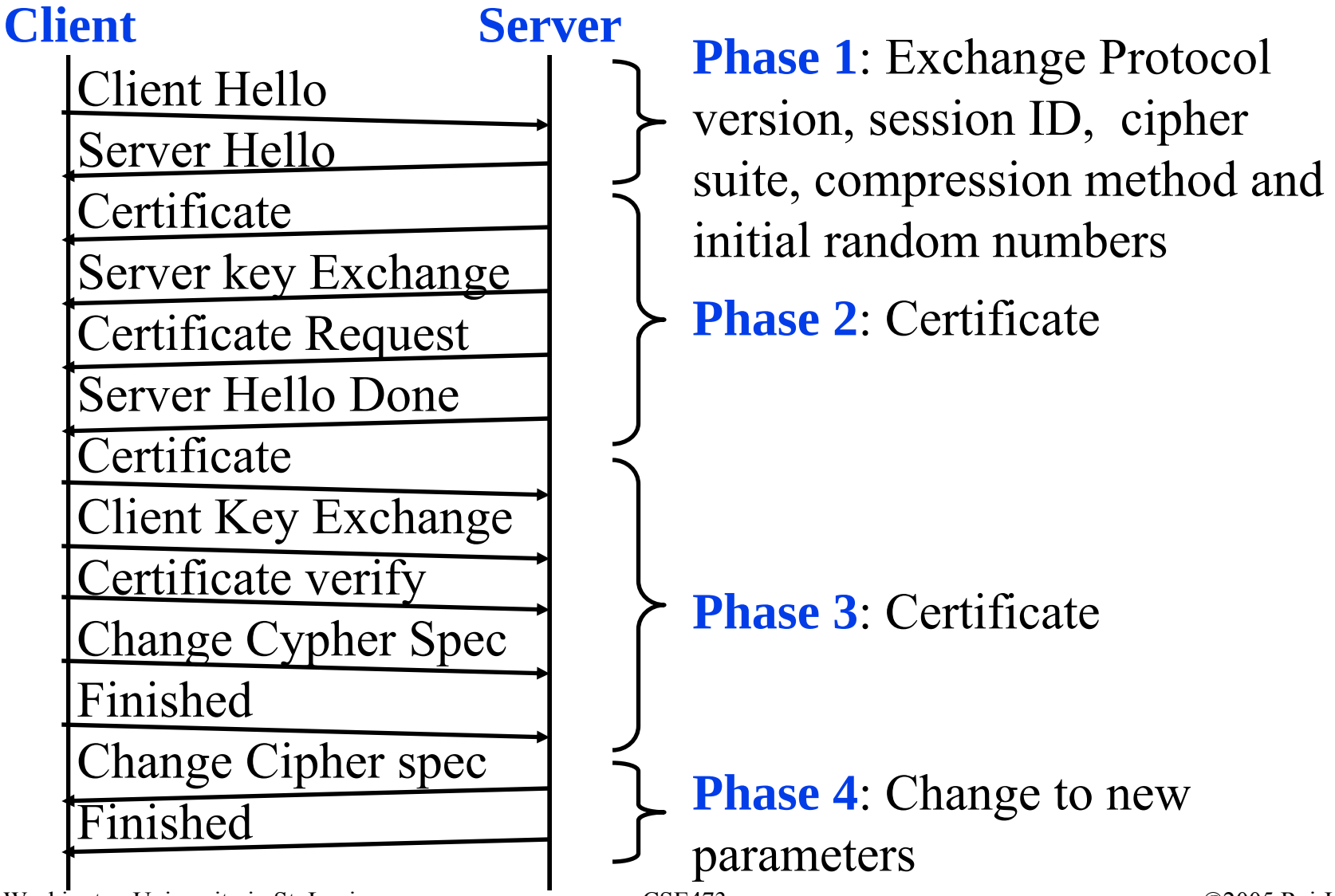
Alert Protocol

- Convey SSL-related alerts to peer entity
- Two bytes
  - First byte: warning(1) or fatal(2)
    - If fatal, SSL immediately terminates connection
    - Other connections on session may continue
    - No new connections on session
  - Second byte indicates specific alert
- Example: Incorrect MAC $\Rightarrow$ fatal alert

Handshake Protocol

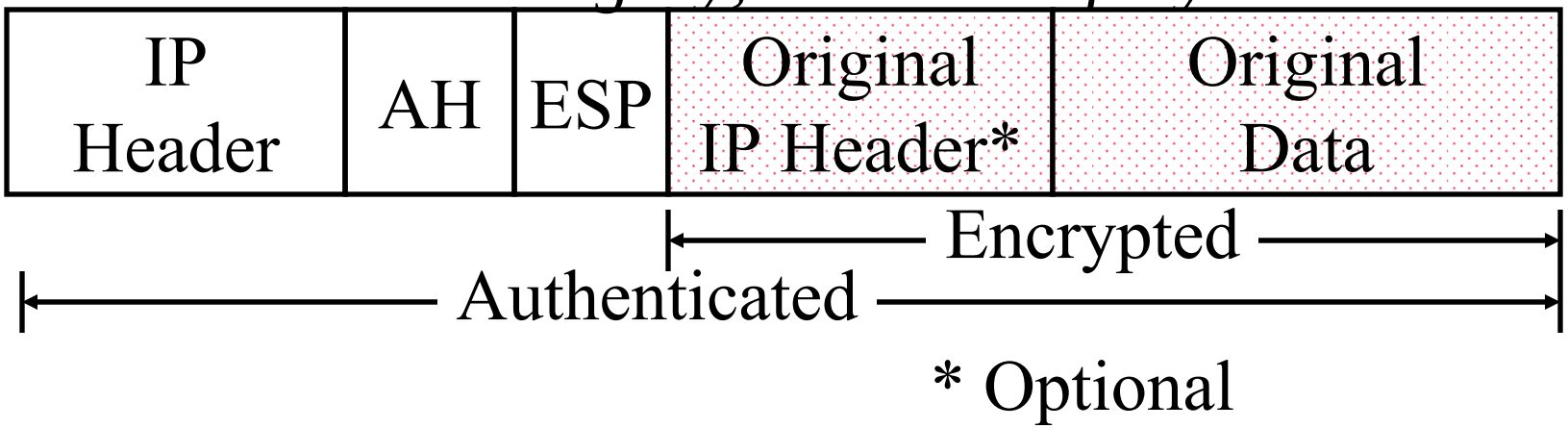
- Negotiate security parameters
- Version: Highest SSL version understood by client
- Random: 28 bytes from secure random number generator
- 32-bit timestamp: Used during key exchange to prevent replay attacks
- Session ID: Variable-length
  - Nonzero ⇒ update existing connection or create new connection on session
  - Zero ⇒ establish new connection on new session
- Cipher Suite: Cryptographic algorithms supported
- Compression Methods supported

Handshake Protocol



IPSec

- Secure IP: A series of proposals from IETF
- Separate Authentication and privacy
- Authentication Header (AH) ensures data *integrity* and *data origin authentication*
- Encapsulating Security Protocol (ESP) ensures *confidentiality, data origin authentication, connectionless integrity, and anti-replay service*



IPSec (Cont)

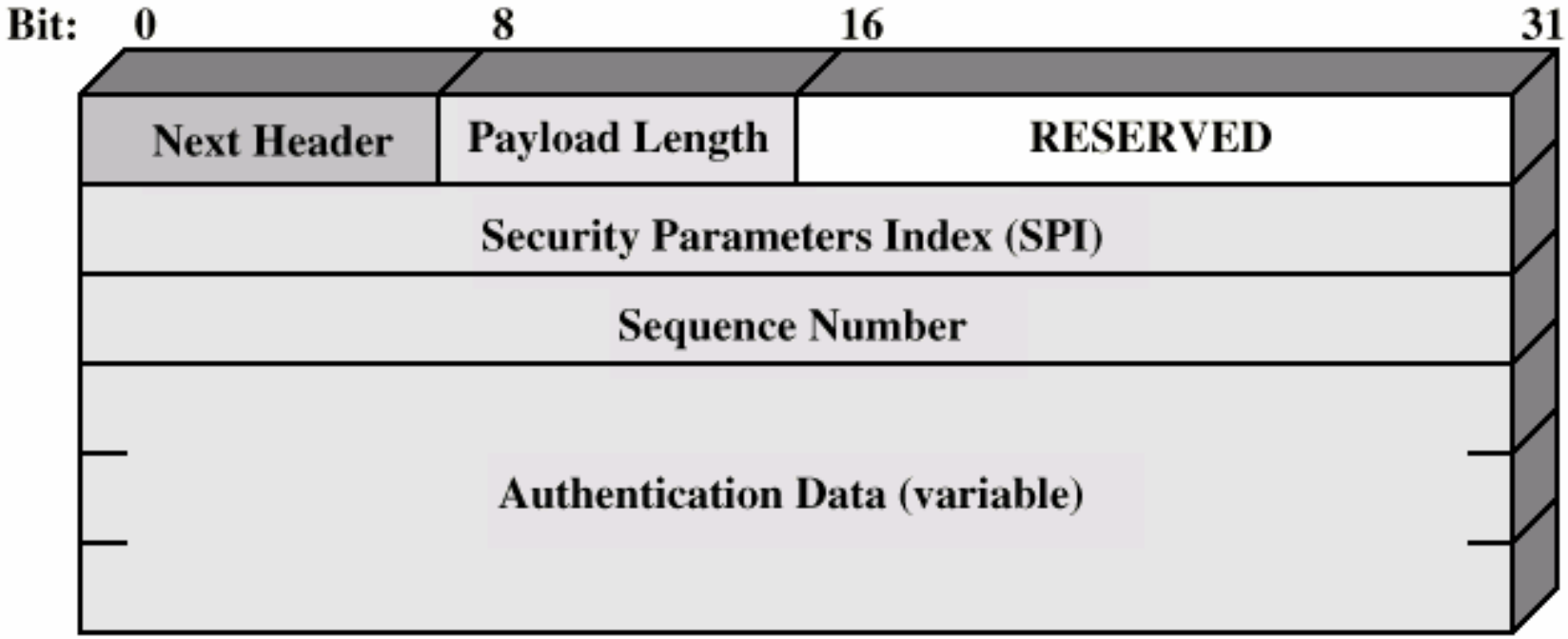
- Two Modes: Tunnel mode, Transport mode
- Tunnel Mode ⇒ Original IP header encrypted
- Transport mode ⇒ Original IP header removed. Only transport data encrypted.
- Supports a variety of encryption algorithms
- Better suited for WAN VPNs (vs Access VPNs)
- A reference implementation (Cerberus) IPSec and interoperability tester are available from NIST

Cerberus = three headed dog guarding the underworld

Security Association

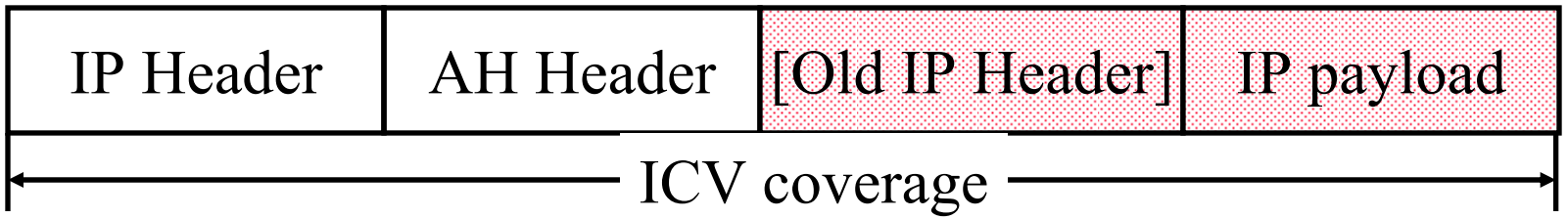
- One way relationship between sender and receiver
- For two way, two associations are required
- Three SA identification parameters
  - Security parameter index
  - IP destination address
  - Security protocol identifier

Authentication Header



- Next Header = TCP, UDP, …
- Payload Length = Length of ***AH*** in 32-bit works − 2 (for IPv4)
  =Length of AH in 64-bit works -1 (for IPv6)
- SPI = Identifies Security association
  (0=Local use, 1-255 reserved)
- Authentication data = Integrity Check Value

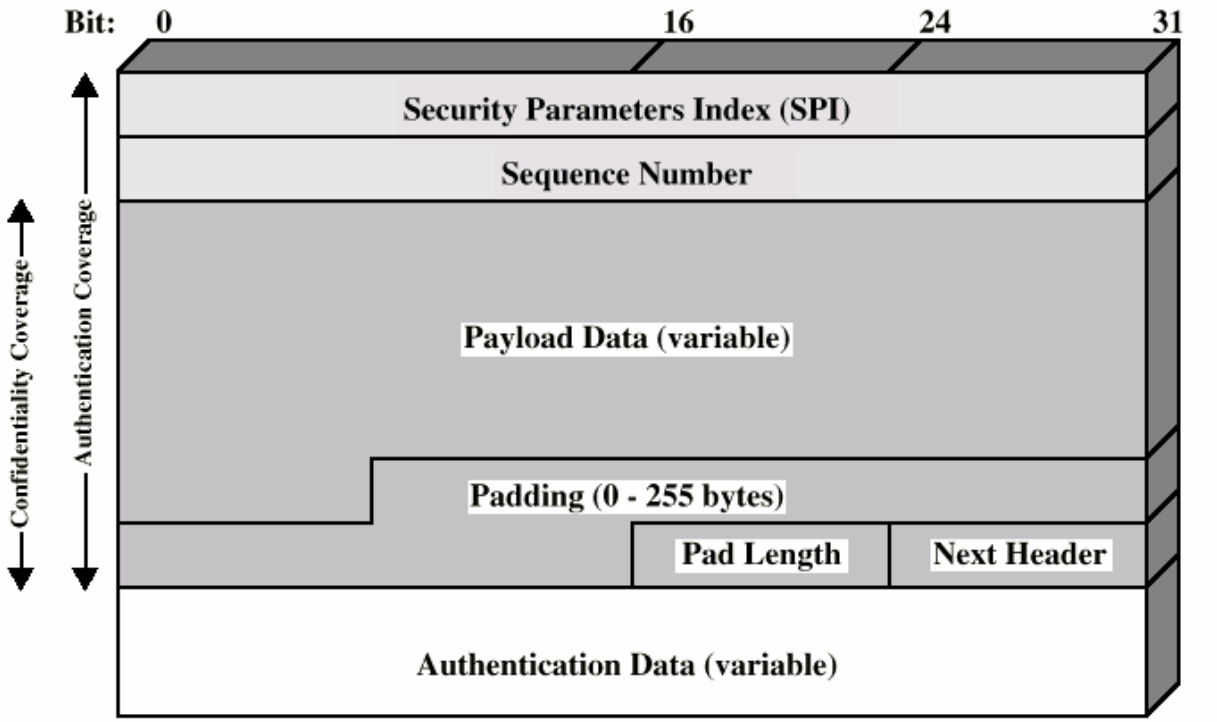
AH ICV Computation



The AH ICV is computed over:

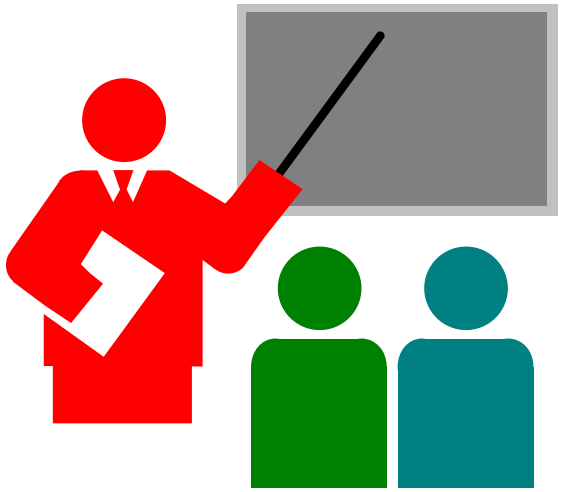
- IP header fields that are either *immutable* in transit or that are *predictable* in value upon arrival at the endpoint for the AH SA, e.g., source address (immutable), destination address with source routing (mutable but predictable)
- The AH header (Next Header, Payload Len, Reserved, SPI, Sequence Number, and the Authentication Data (which is set to zero for this computation), and explicit padding bytes (if any))
- The upper level protocol data, which is assumed to be immutable in transit

ESP Packet



- Payload data: IP, TCP, UDP packet
- Pad Length in bytes
- Next Header: Type of payload (TCP, UDP, …)
- Authentication Data: Integrity Check Value over ESP packet

Summary



- DES and 3DES are out. AES is current standard for encryption
- SHA-1 is older secure hash function
- SSL provides security at the session layer
- IPSec provides authentication and/or encryption

Reading Assignment

- Read Chapter 21 of Stallings 7th edition
  Read 2402 (AH), RFC 2406 (ESP)

Homework

- Submit answer to Exercise 21.13a in Stallings' 7th edition