

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/>



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

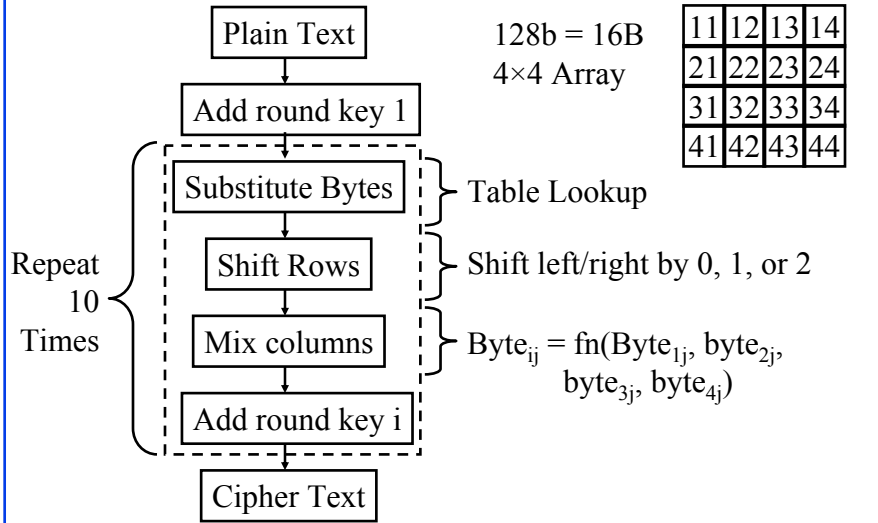
DES and 3DES

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

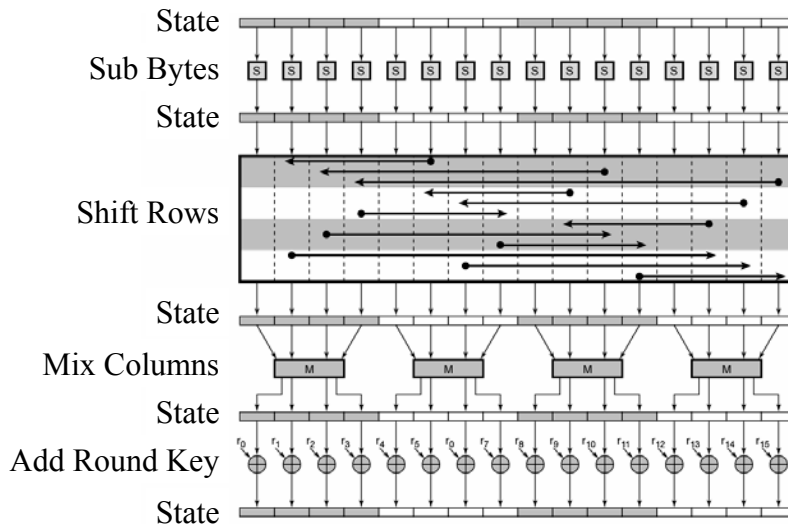
Advanced Encryption Standard (AES)

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

AES (cont)

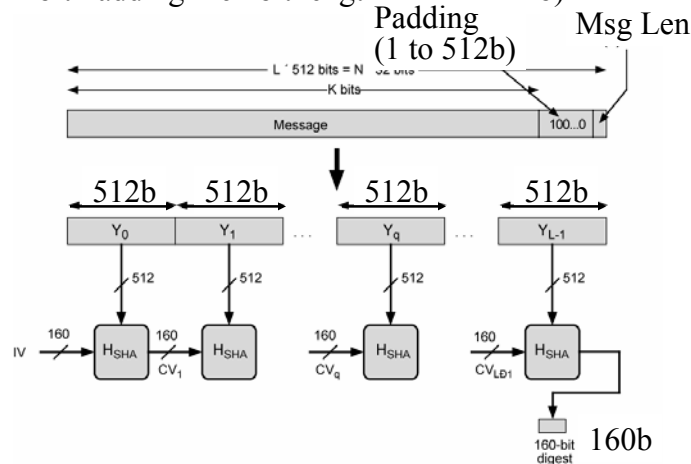


AES Encryption Round



Secure Hash Algorithm 1 (SHA-1)

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



Washington University in St. Louis

CSE473s

©2005 Raj Jain

18-7

SSL and TLS

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

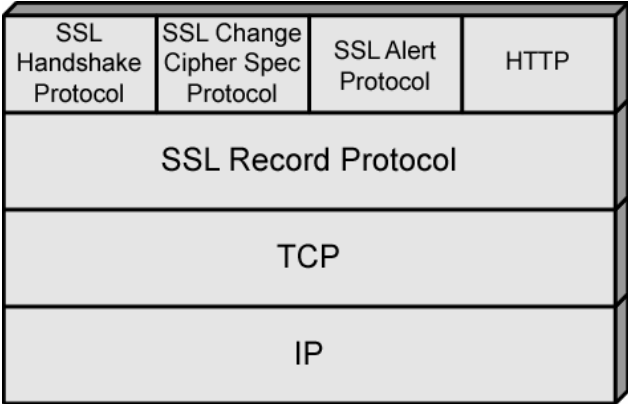
Washington University in St. Louis

CSE473s

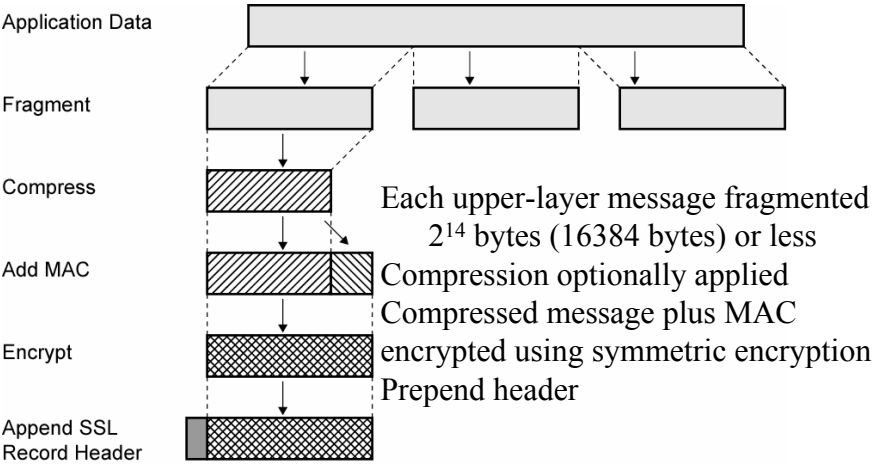
©2005 Raj Jain

18-8

SSL Protocol Stack



SSL Record Protocol Operation



Record Protocol Header

Content Type	Major Version	Minor Version	Compressed Length	Data
8b	8b	8b	16b	

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

Change Cipher Spec Protocol

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

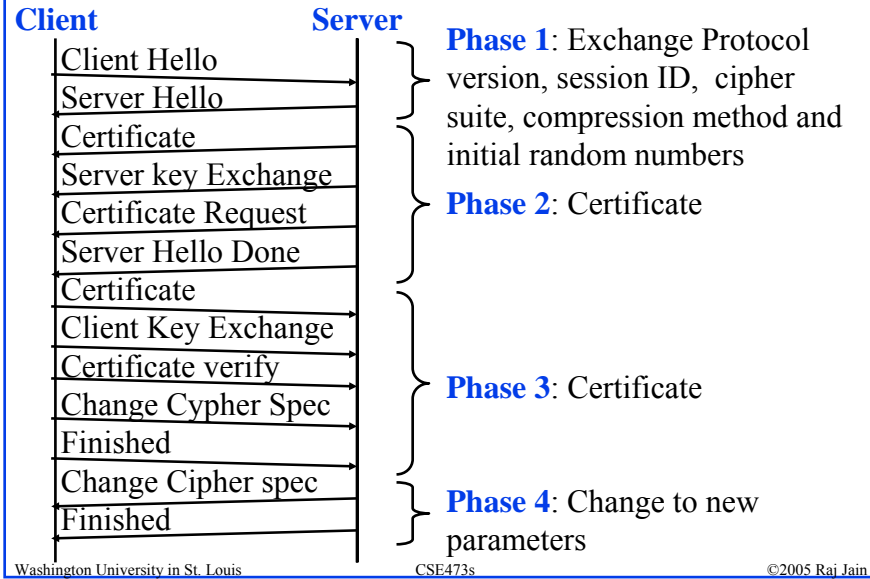
Alert Protocol

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

Handshake Protocol

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

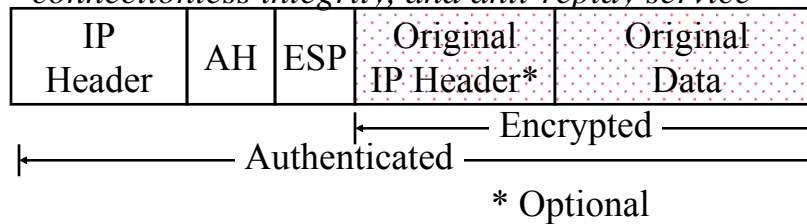
Handshake Protocol



18-15

IPSec

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



Washington University in St. Louis CSE473s ©2005 Raj Jain

18-16

IPSec (Cont)

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

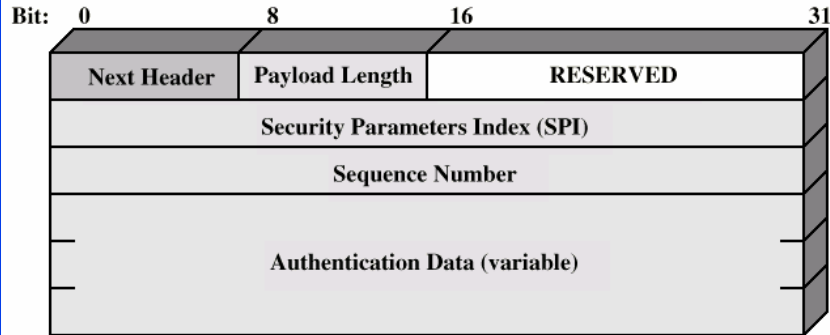


Cerberus = three headed dog guarding the underworld

Security Association

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

Authentication Header



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

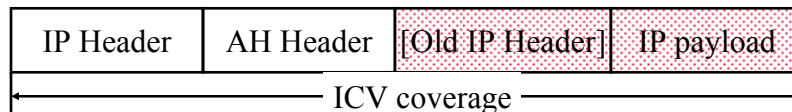
Washington University in St. Louis

CSE473s

©2005 Raj Jain

18-19

AH ICV Computation



The AH ICV is computed over:

- q 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)
- q 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))
- q The upper level protocol data, which is assumed to be immutable in transit

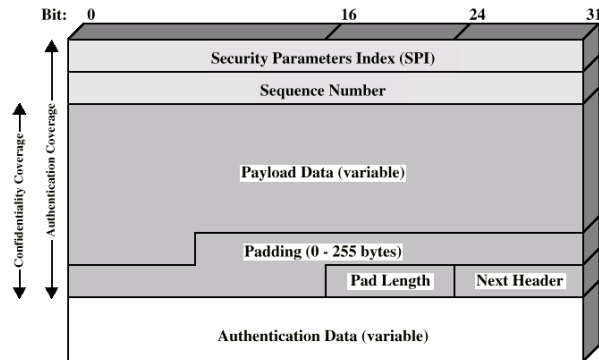
Washington University in St. Louis

CSE473s

©2005 Raj Jain

18-20

ESP Packet



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

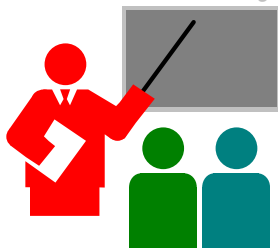
Washington University in St. Louis

CSE473s

©2005 Raj Jain

18-21

Summary



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

Washington University in St. Louis

CSE473s

©2005 Raj Jain

18-22

Reading Assignment

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

Homework

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