William Stallings Data and Computer Communications

Ch.18 Network Security

Hoon-Jae Lee

hjlee@dongseo.ac.kr

Security Requirements

- Confidentiality
- Integrity
- Availability

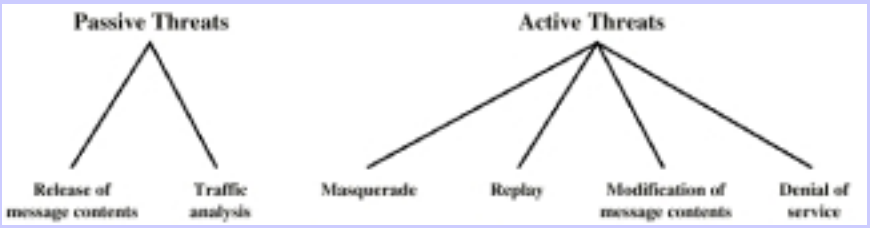
Passive Attacks

- Eavesdropping on transmissions
- To obtain information
- Release of message contents
  - Outsider learns content of transmission
- Traffic analysis
  - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- Difficult to detect
- Can be prevented

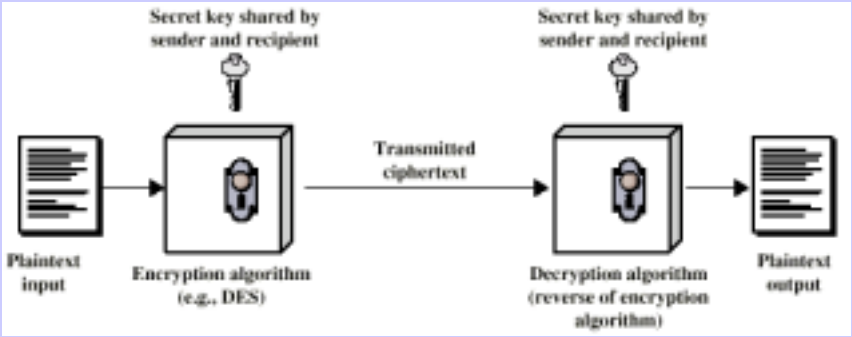
Active Attacks

- Masquerade
  - Pretending to be a different entity
- Replay
- Modification of messages
- Denial of service
- Easy to detect
  - Detection may lead to deterrent
- Hard to prevent

Security Threats



Conventional Encryption



Ingredients

- Plain text
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

Requirements for Security

- Strong encryption algorithm
  - Even if known, should not be able to decrypt or work out key
  - Even if a number of cipher texts are available together with plain texts of them
- Sender and receiver must obtain secret key securely
- Once key is known, all communication using this key is readable

Attacking Encryption

- Crypt analysis
  - Relay on nature of algorithm plus some knowledge of general characteristics of plain text
  - Attempt to deduce plain text or key
- Brute force
  - Try every possible key until plain text is achieved

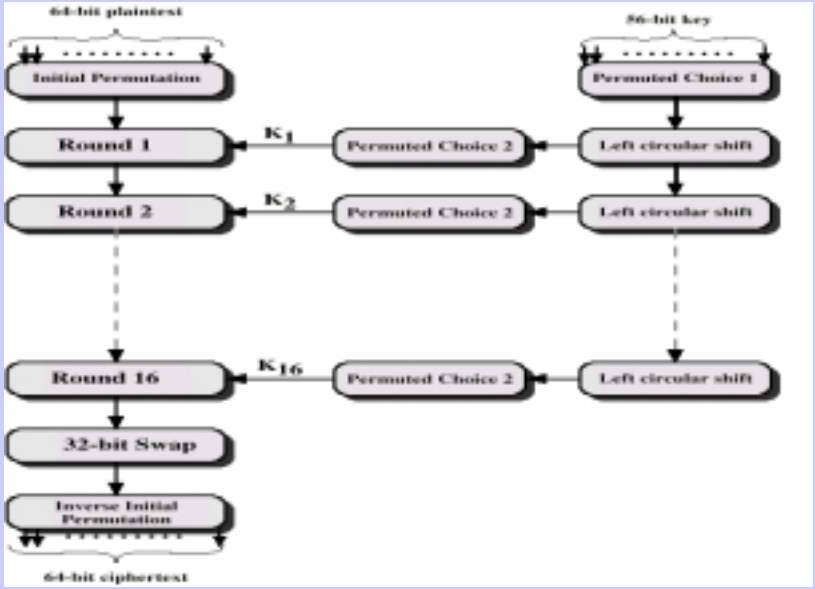
Algorithms

- Block cipher
  - Process plain text in fixed block sizes producing block of cipher text of equal size
  - Data encryption standard (DES)
  - Triple DES (TDES)

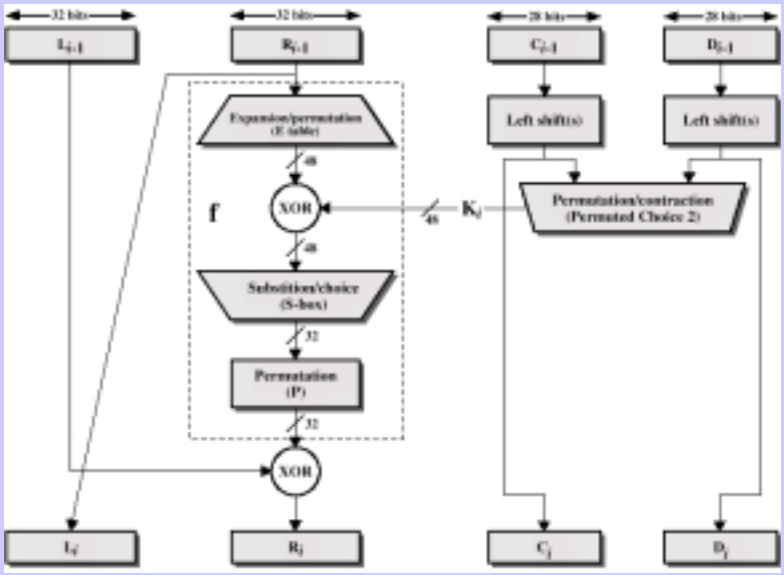
Data Encryption Standard

- US standard
- 64 bit plain text blocks
- 56 bit key

DES Encryption Algorithm



DES Single Iteration



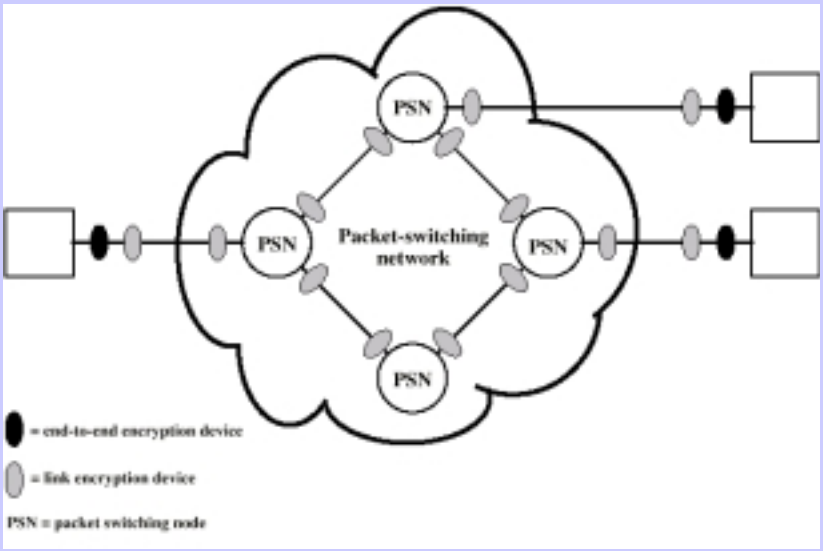
Strength of DES

- Declared insecure in 1998
- Electronic Frontier Foundation
- DES Cracker machine
- DES now worthless
- Alternatives include TDEA

Triple DEA

- ANSI X9.17 (1985)
- Incorporated in DEA standard 1999
- Uses 3 keys and 3 executions of DEA algorithm
- Effective key length 168 bit

Location of Encryption Devices



Link Encryption

- Each communication link equipped at both ends
- All traffic secure
- High level of security
- Requires lots of encryption devices
- Message must be decrypted at each switch to read address (virtual circuit number)
- Security vulnerable at switches
  - Particularly on public switched network

End to End Encryption

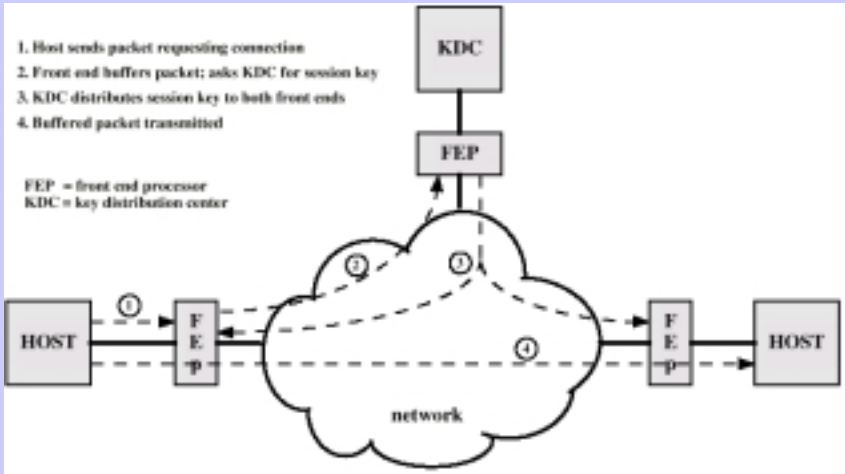
- Encryption done at ends of system
- Data in encrypted form crosses network unaltered
- Destination shares key with source to decrypt
- Host can only encrypt user data
  - Otherwise switching nodes could not read header or route packet
- Traffic pattern not secure

- Use both link and end to end

Key Distribution

- Key selected by A and delivered to B
- Third party selects key and delivers to A and B
- Use old key to encrypt and transmit new key from A to B
- Use old key to transmit new key from third party to A and B

Automatic Key Distribution (diag)



Automatic Key Distribution

- Session Key
  - Used for duration of one logical connection
  - Destroyed at end of session
  - Used for user data
- Permanent key
  - Used for distribution of keys
- Key distribution center
  - Determines which systems may communicate
  - Provides one session key for that connection
- Front end processor
  - Performs end to end encryption
  - Obtains keys for host

Traffic Padding

- Produce cipher text continuously
- If no plain text to encode, send random data
- Make traffic analysis impossible

Message Authentication

- Protection against active attacks
  - Falsification of data
  - Eavesdropping
- Message is authentic if it is genuine and comes from the alleged source
- Authentication allows receiver to verify that message is authentic
  - Message has not altered
  - Message is from authentic source
  - Message timeline

Authentication Using Encryption

- Assumes sender and receiver are only entities that know key
- Message includes:
  - error detection code
  - sequence number
  - time stamp

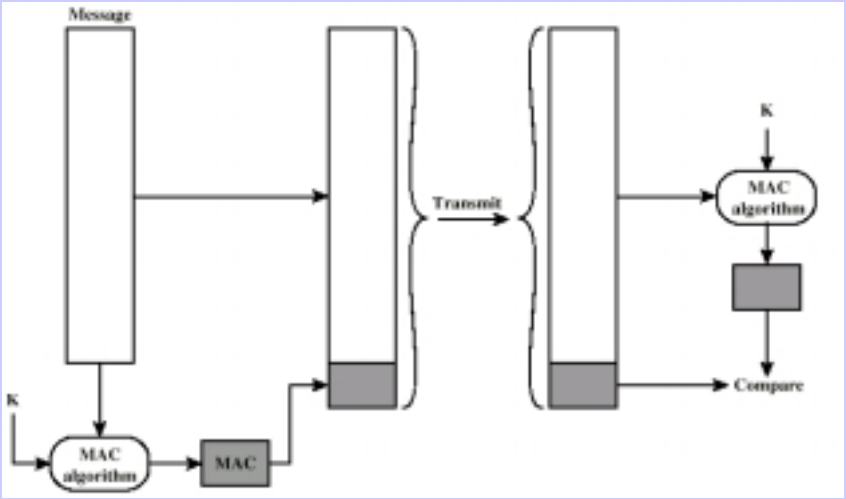
Authentication Without Encryption

- Authentication tag generated and appended to each message
- Message not encrypted
- Useful for:
  - Messages broadcast to multiple destinations
    - ✓ Have one destination responsible for authentication
  - One side heavily loaded
    - ✓ Encryption adds to workload
    - ✓ Can authenticate random messages
  - Programs authenticated without encryption can be executed without decoding

Message Authentication Code

- Generate authentication code based on shared key and message
- Common key shared between A and B
- If only sender and receiver know key and code matches:
  - Receiver assured message has not altered
  - Receiver assured message is from alleged sender
  - If message has sequence number, receiver assured of proper sequence

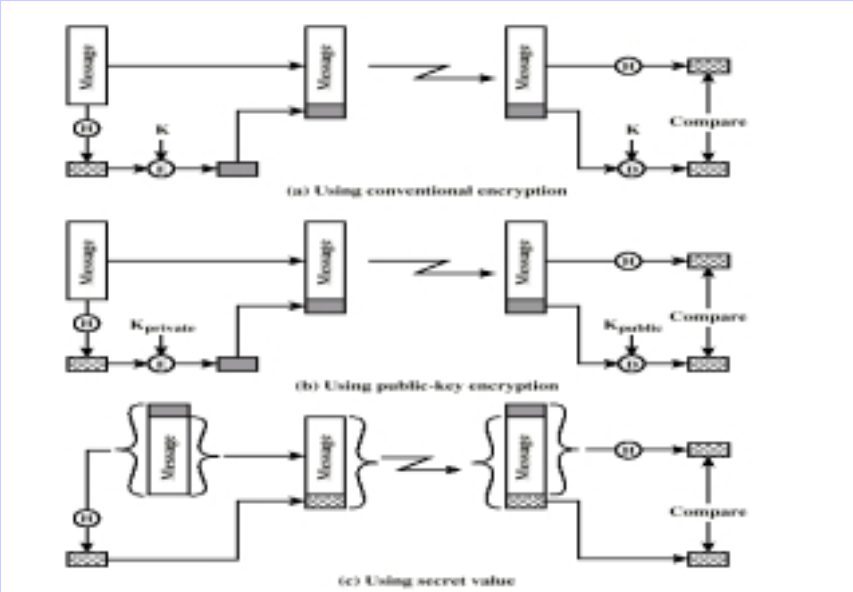
Message Authentication Using Message Authentication Code



One Way Hash Function

- Accepts variable size message and produces fixed size tag (message digest)
- Advantages of authentication without encryption
  - Encryption is slow
  - Encryption hardware expensive
  - Encryption hardware optimized to large data
  - Algorithms covered by patents
  - Algorithms subject to export controls (from USA)

Using One Way Hash



Secure Hash Functions

- Hash function must have following properties:
  - Can be applied to any size data block
  - Produce fixed length output
  - Easy to compute
  - Not feasible to reverse
  - Not feasible to find two message that give the same hash

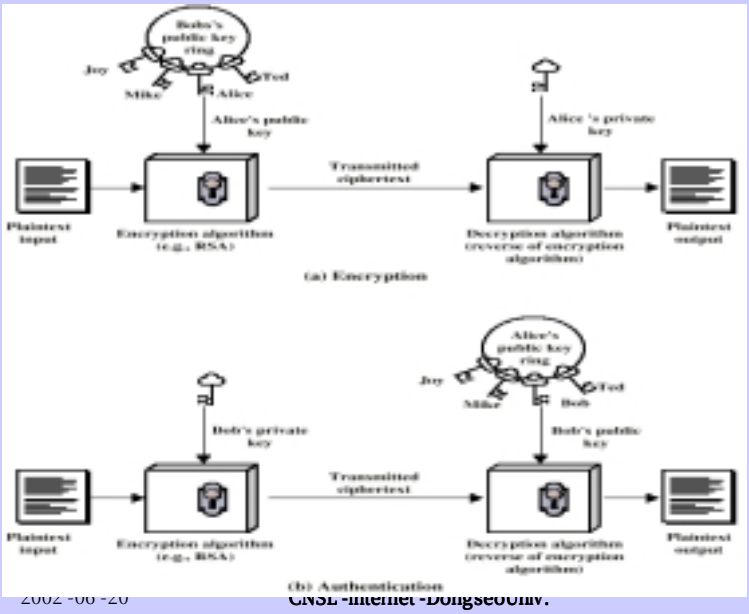
SHA -1

- Secure Hash Algorithm 1
- Input message less than 2^{64} bits
  - Processed in 512 bit blocks
- Output 160 bit digest

Public Key Encryption

  - Decryption algorithm
- Based on mathematical algorithms
- Asymmetric
  - Use two separate keys
- Ingredients
  - Plain text
  - Encryption algorithm
  - Public and private key
  - Cipher text

Public Key Encryption (diag)



Public Key Encryption - Operation

- One key made public
  - Used for encryption
- Other kept private
  - Used for decryption
- Infeasible to determine decryption key given encryption key and algorithm
- Either key can be used for encryption, the other for decryption

Steps

- User generates pair of keys
- User places one key in public domain
- To send a message to user, encrypt using public key
- User decrypts using private key

Digital Signature

- Sender encrypts message with their private key
- Receiver can decrypt using sneders public key
- This authenticates sender, who is only person who has the matching key
- Does not give privacy of data
  - Decrypt key is public

RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

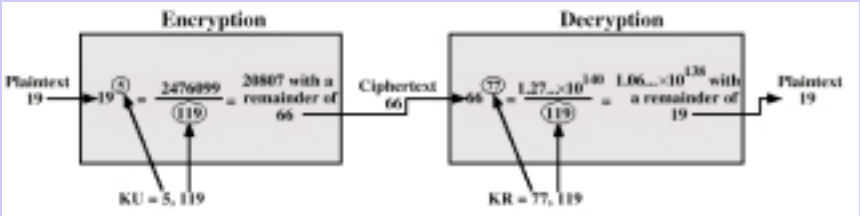
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

RSA Example



IPv4 and IPv6 Security

- IPSec
- Secure branch office connectivity over Internet
- Secure remote access over Internet
- Extranet and intranet connectivity
- Enhanced electronic commerce security

IPSec Scope

- Authentication header
- Encapsulated security payload
- Key exchange
- RFC 2401,2402,2406,2408

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

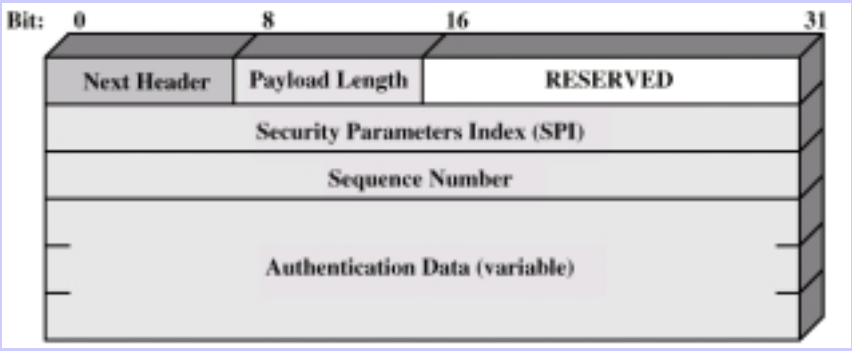
SA Parameters

- Sequence number counter
- Sequence counter overflow
- Anti -reply windows
- AH information
- ESP information
- Lifetime of this association
- IPSec protocol mode
  - Tunnel, transport or wildcard
- Path MTU

Transport and Tunnel Modes

- Transport mode
  - Protection for upper layer protocols
  - Extends to payload of IP packet
  - End to end between hosts
- Tunnel mode
  - Protection for IP packet
  - Entire packet treated as payload for outer IP "packet"
  - No routers examine inner packet
  - May have different source and destination address
  - May be implemented at firewall

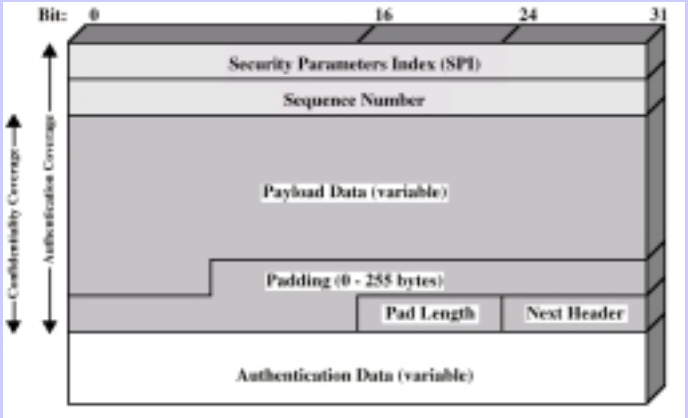
Authentication Header



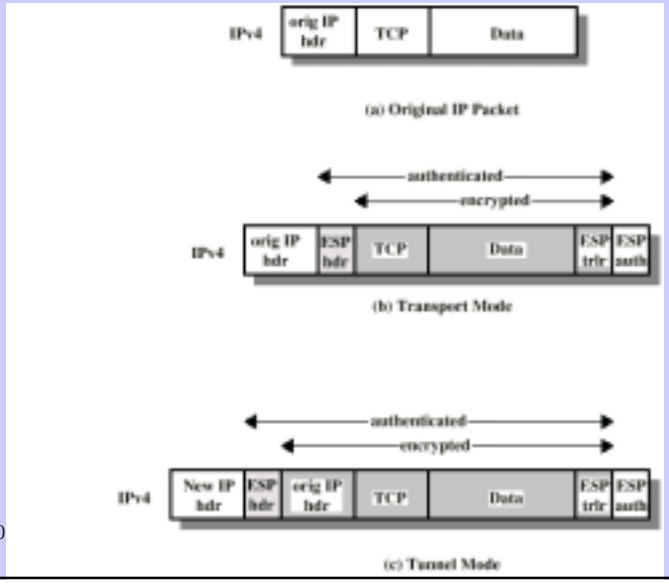
Encapsulating Security Payload

- ESP
- Confidentiality services

ESP Packet



Scope of ESP



Key Management

- Manual
- Automatic
  - ISAKMP/Oakley
    - ✓Oakley key determination protocol
    - ✓Internet security association and key management protocol