1. Security Requirements and Attacks

- computer security and network security and cryptography
- three requirements:
  - secrecy/integrity/availability(/authentication)
- security threats
  - interruption/interception/modification/fabricatio n

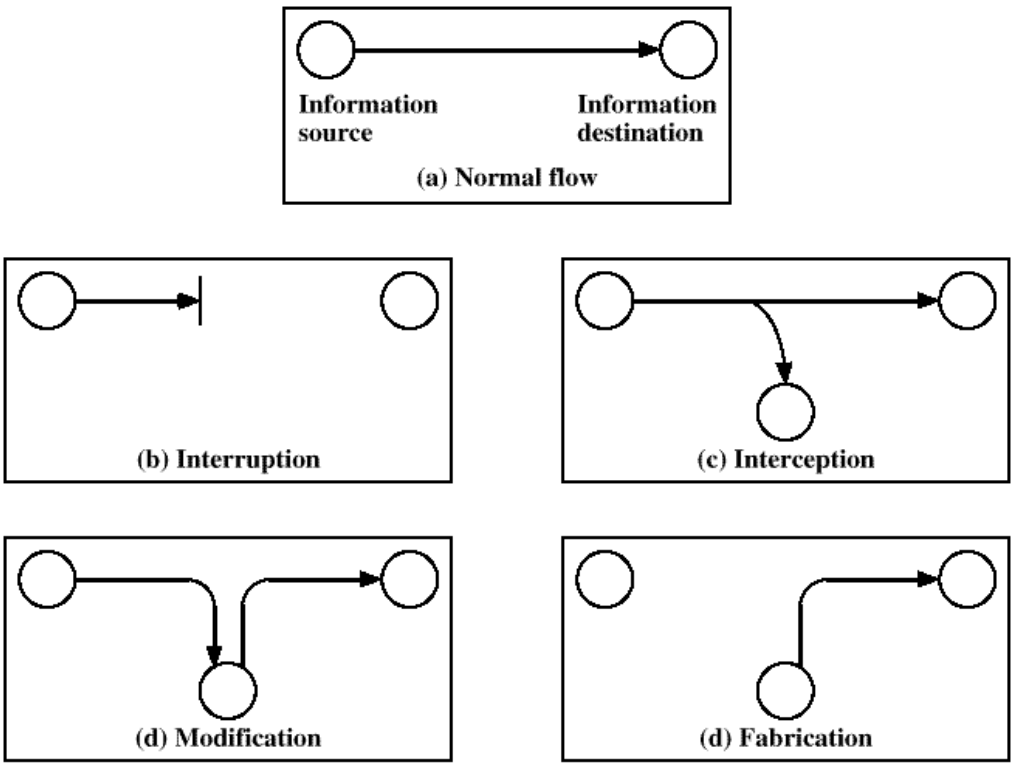


Figure 18.1 Security Threats

- passive attack
  - release-of-message contents/traffic analysis
  - detect vs. prevent
- active attack
  - masquerade/replay/modification of messages/denial of service
  - prevent vs. detect

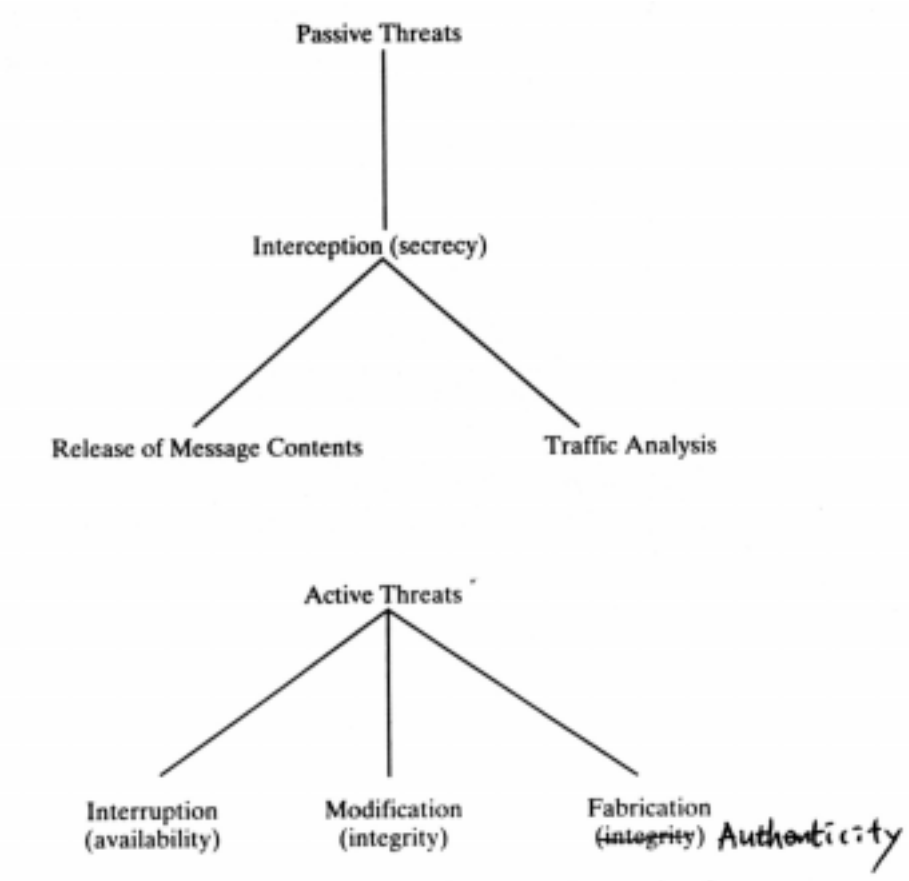


FIGURE 18.2 Active and passive network security threats.

- Conventional encryption
  - plaintext/ciphertext/encryption algorithm/key
  - security factor
    - encryption algorithm
    - key
  - representation
    - encryption: $Y = E_K(X)$
    - decryption: $X = D_K(Y)$

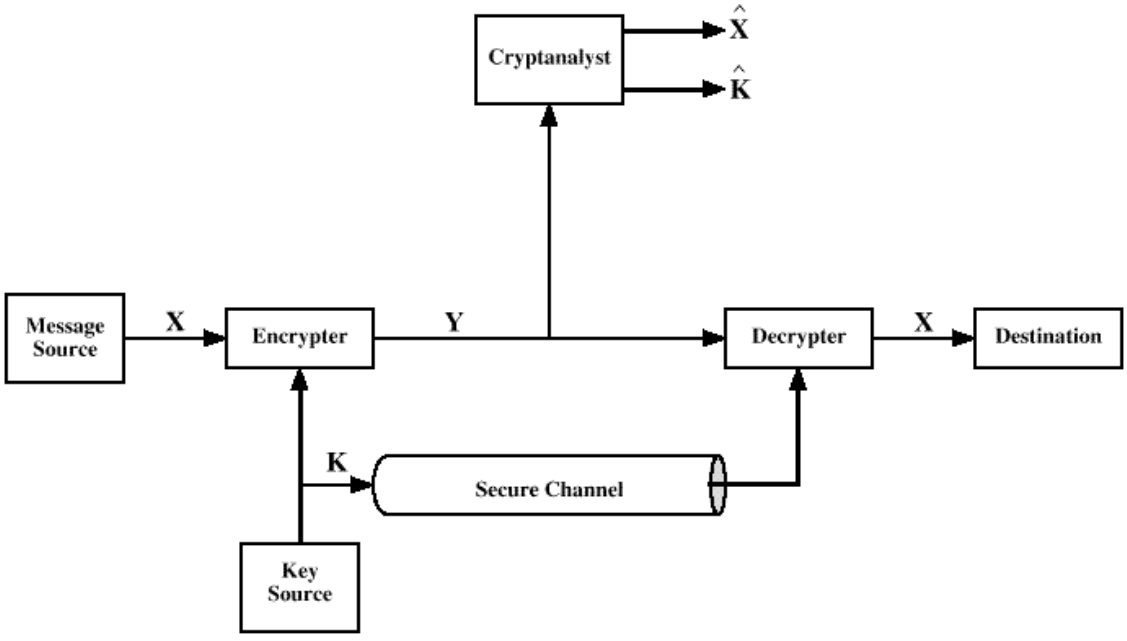


Figure 18.3 Model of Conventional Cryptosystem

- Encryption algorithms
  - the Data Encryption Standard(DES)
    - block cipher
    - NBS(National Bureau of Standards) adopted DES as Federal Information Processing Standard 46(FIPS PUB 46) in 1977
    - NIST(National Institute of Standards and Technology) “reaffirmed” DES for federal use for another five years in 1994
    - block size = 64bits, key size = 56 bits
    - overall encryption process
      - 1. 64-bit plaintext passes through an initial permutation(IP)
      - 2. 16 iterations of the same function
      - 3. The preoutput is passed through an inverse of the initial permutation
    - decryption process
      - use the ciphertext as input to the DES algorithm, but use the keys in reverse order

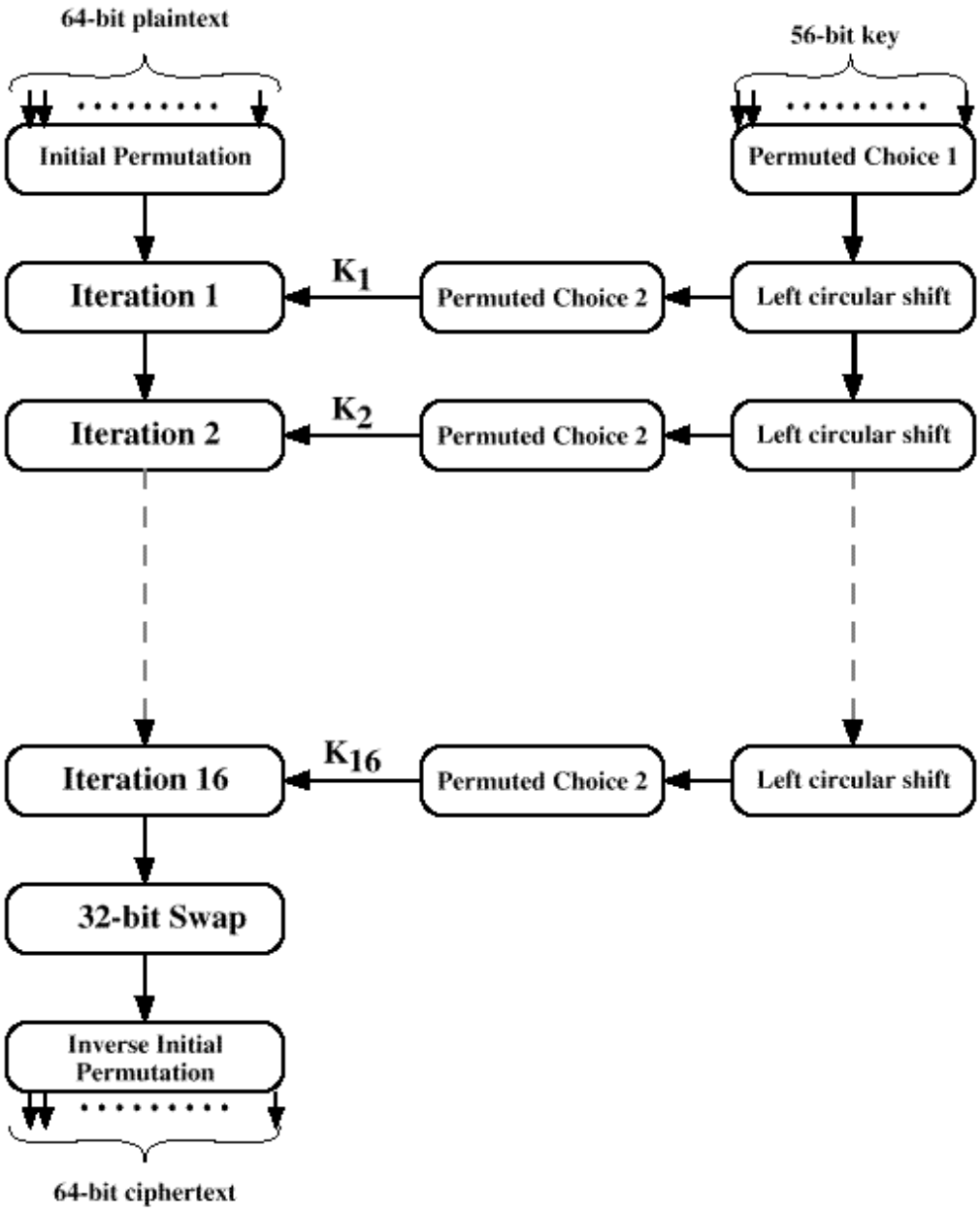


Figure 18.4 General Depiction of DES Algorithm

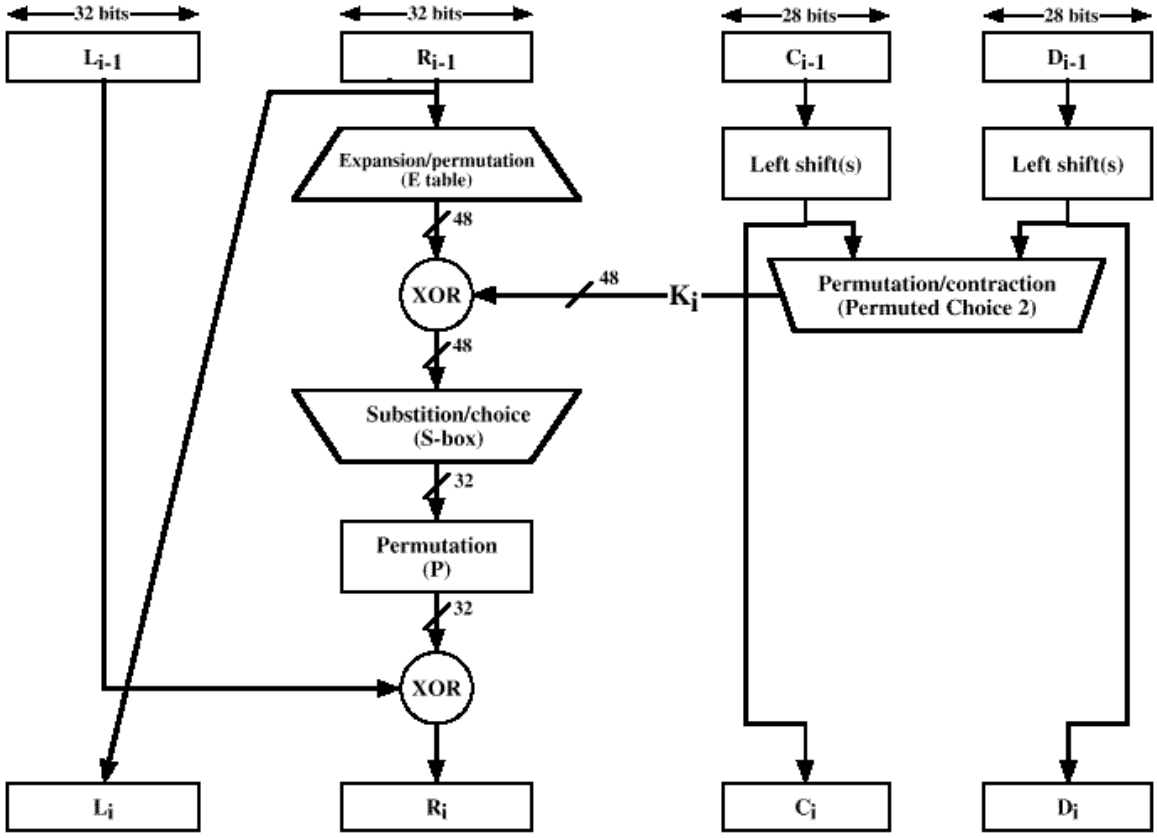


Figure 18.5 Single Iteration of DES Algorithm

- the strength of DES
  - level of security provided by DES
    - the nature of the algorithm
      - eight substitution tables, or S-boxes

        the design criteria for these boxes have never been made public -> trapdoor suspicion
      - extensive scrutiny -> one of the strongest encryption algorithms
    - the key size
      - 7x10^16 possible keys: a brute-force attack appears impractical:

        one DES encryption/microsecond would take more than a thousand years(Chinese radio attack)
  - 1977
    - Diffie and Hellman postulated
    - one million keys per second/ $20 million in 1977 dollars
  - 1993
    - Wiener used pipeline technique
    - 50 million keys per second * 5760 /$100,000 -> 35 hours
  - the time has come to investigate alternatives for conventional encryption -> triple DES

- triple DES
  - Tuchman proposed in 1979
  - two keys and three executions
    - C=Ek1[Dk2[Ek1[p]]]
      - allows users of triple DES to decrypt data encrypted by users of the older, single DES
  - it turns out that there is a simple technique, known as a meet-in-the-middle attack, that would reduce a double DES system with two keys to the relative strength of ordinary single DES
  - effective key length is 112 bits

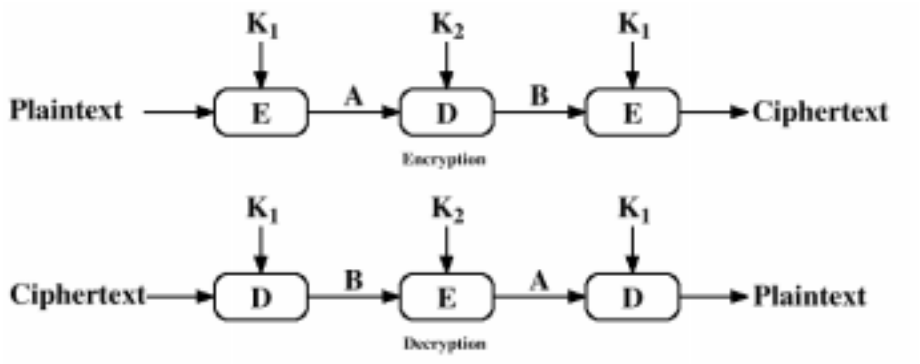


Figure 18.6 Triple DES

- Location of encryption devices
  - link encryption
  - end-to-end encryption

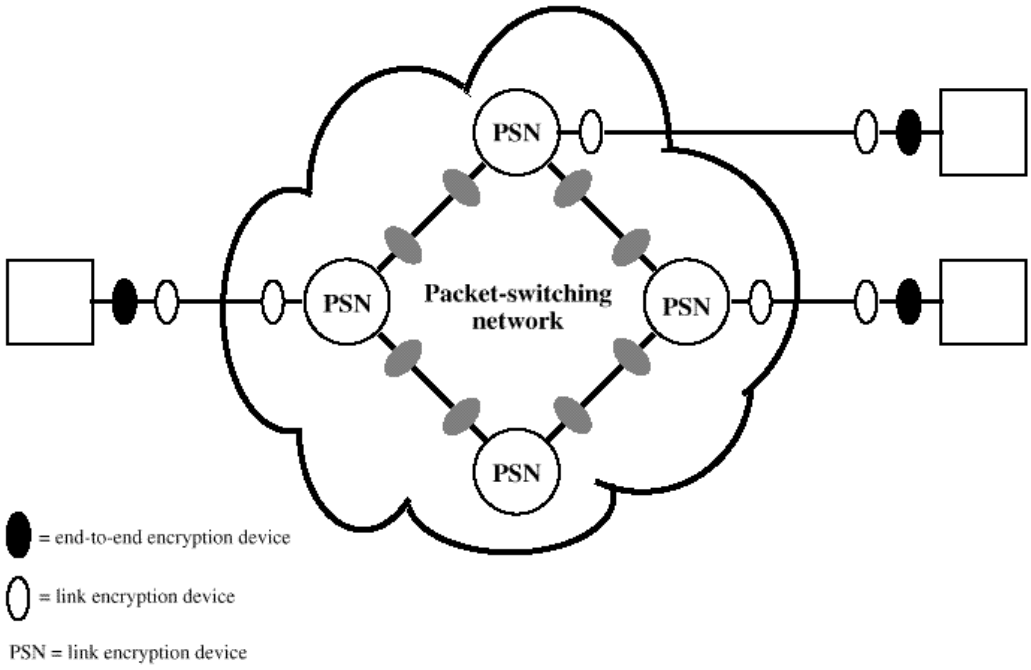


Figure 18.7 Encryption Across a Packet-Switching Network

- Key distribution
  - the strength of any cryptographic system rests with the key distribution technique(Fig18.8)
    - 1. A selects a key and delivers to B
      - physically/using old key
    - 2. a third party selects a key and delivers to A and B
      - physically/using old key

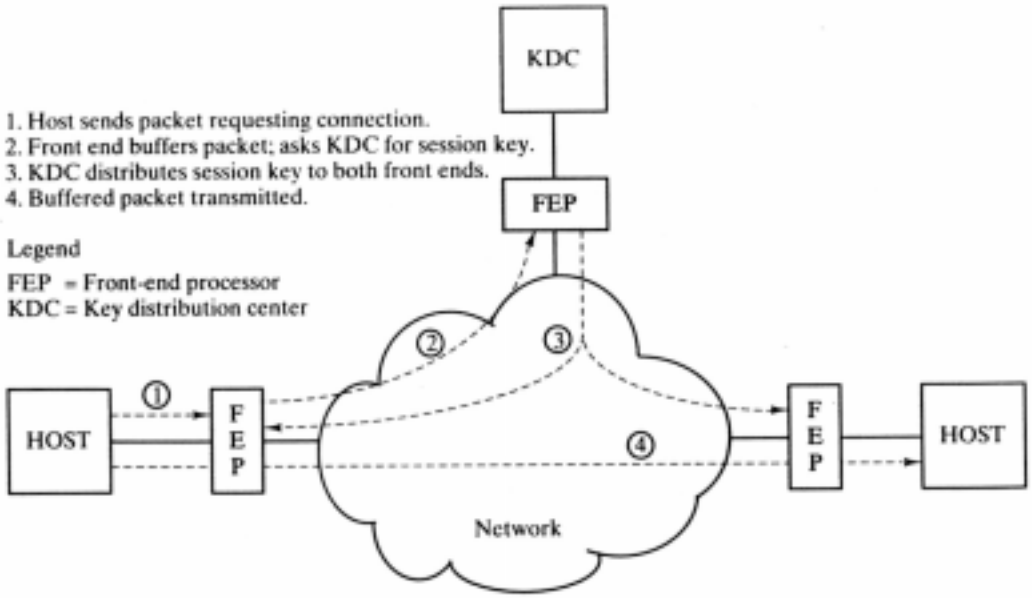
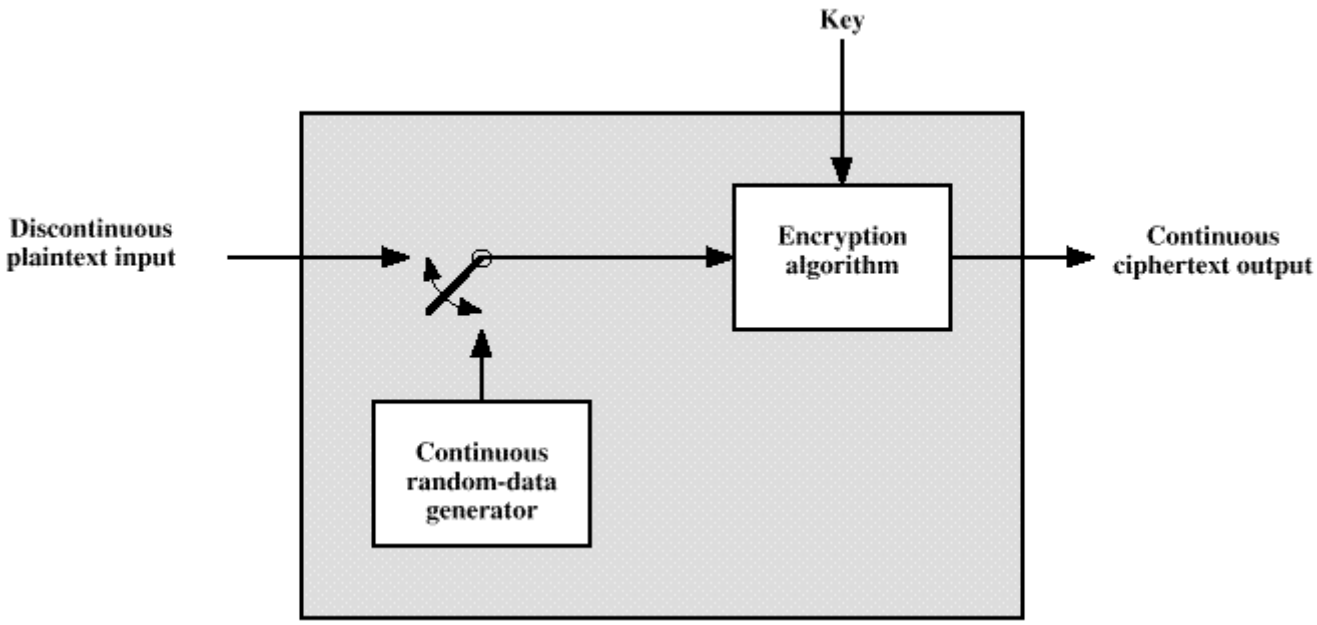


FIGURE 18.8 Automatic key distribution for connection-oriented protocol.

- Traffic padding
  - assess the amount of traffic on a network
  - observe the amount of traffic entering and leaving each end system



3. Message Authentication and Hash Functions

- Approaches to message authentication
  - two aspects
    - the contents
    - the source
  - authentication using conventional encryption
    - simple
    - possible to use
      - error detection code
      - a sequence number
      - timestamp
  - message authentication without message encryption
    - three situations
      - broadcasting
      - heavy loading
      - computer program

– message authentication code

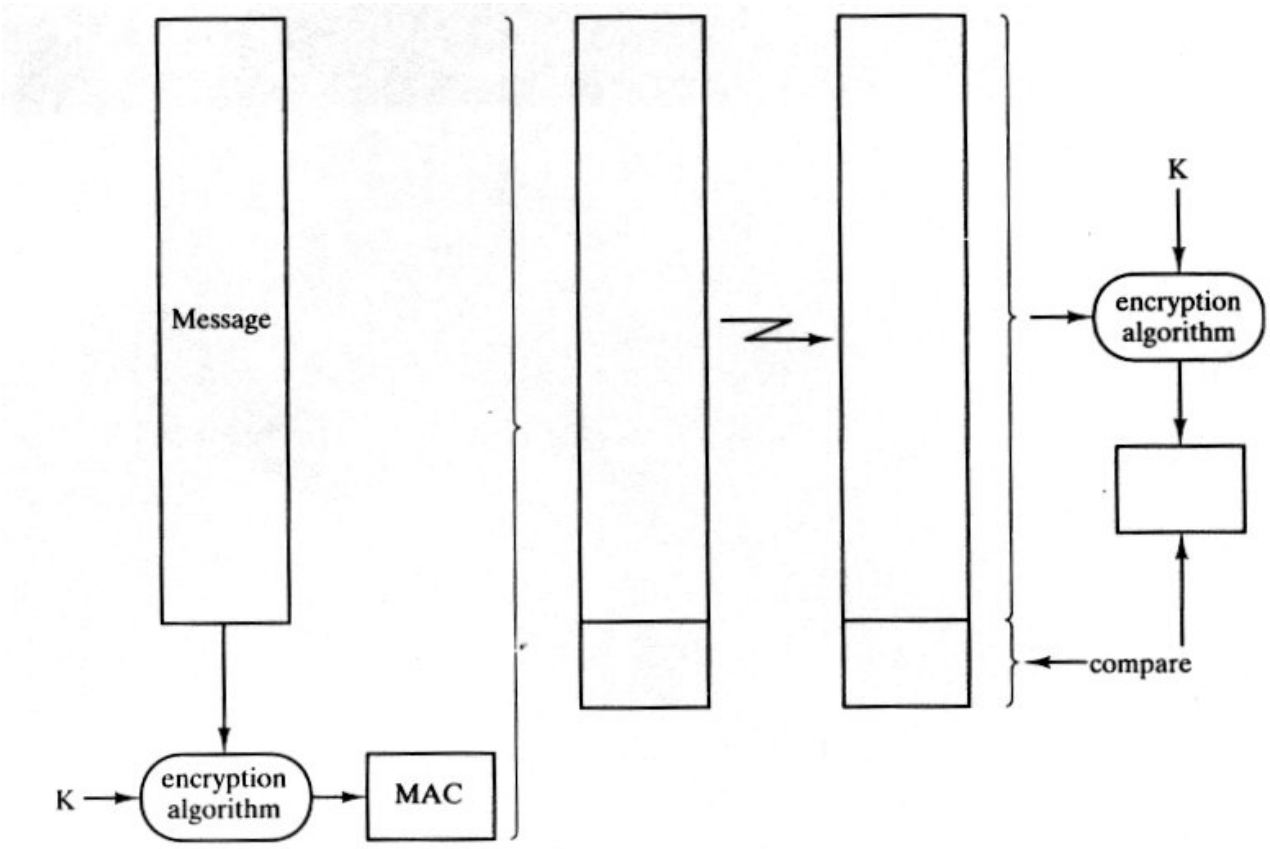
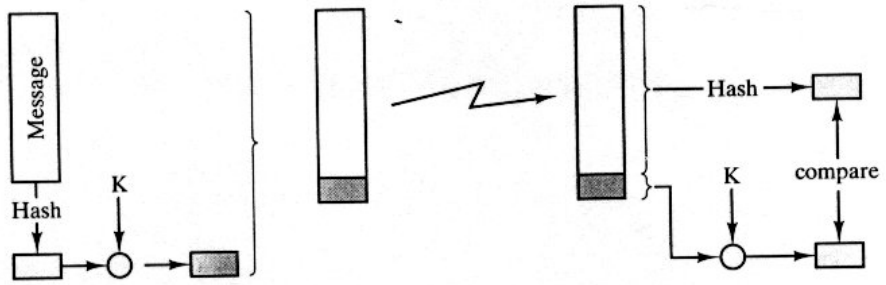
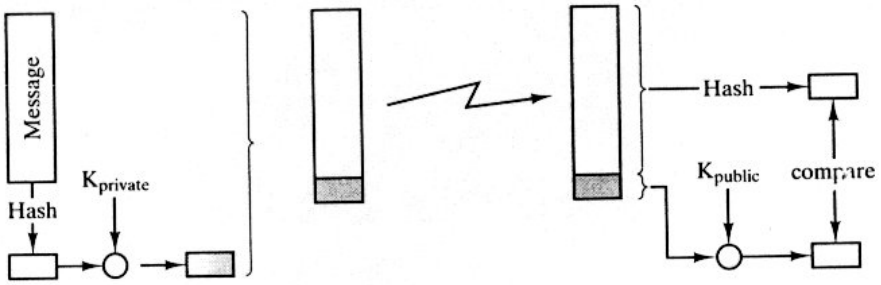


FIGURE 18.10 Message authentication using a message authentication code (MAC).

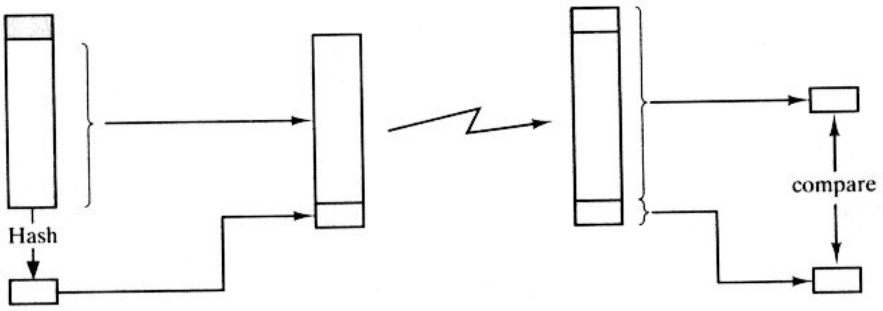
- one-way hash function
  - message digest, fingerprint
  - avoid encryption altogether
    - software speed
    - hardware cost/optimization
    - algorithm patent/export control
  - three ways



(a) Using conventional encryption



(b) Using public-key encryption



(c) Using secret value

FIGURE 18.11 Message authentication using a one-way hash function.

- Secure hash functions
  - hash function requirements
    - input size
    - output size
    - efficiency
    - weak one-way property
    - strong one-way property
    - collision-freeness
      - to protect birthday attack
  - simple hash functions
    - bit-by-bit XOR

- MD5 algorithm description
  - by Ron Rivest
  - 128-bit message digest
  - procedure
    - append padding bits
    - append length
    - initialize MD buffer
    - process message in 512-bit blocks
    - output

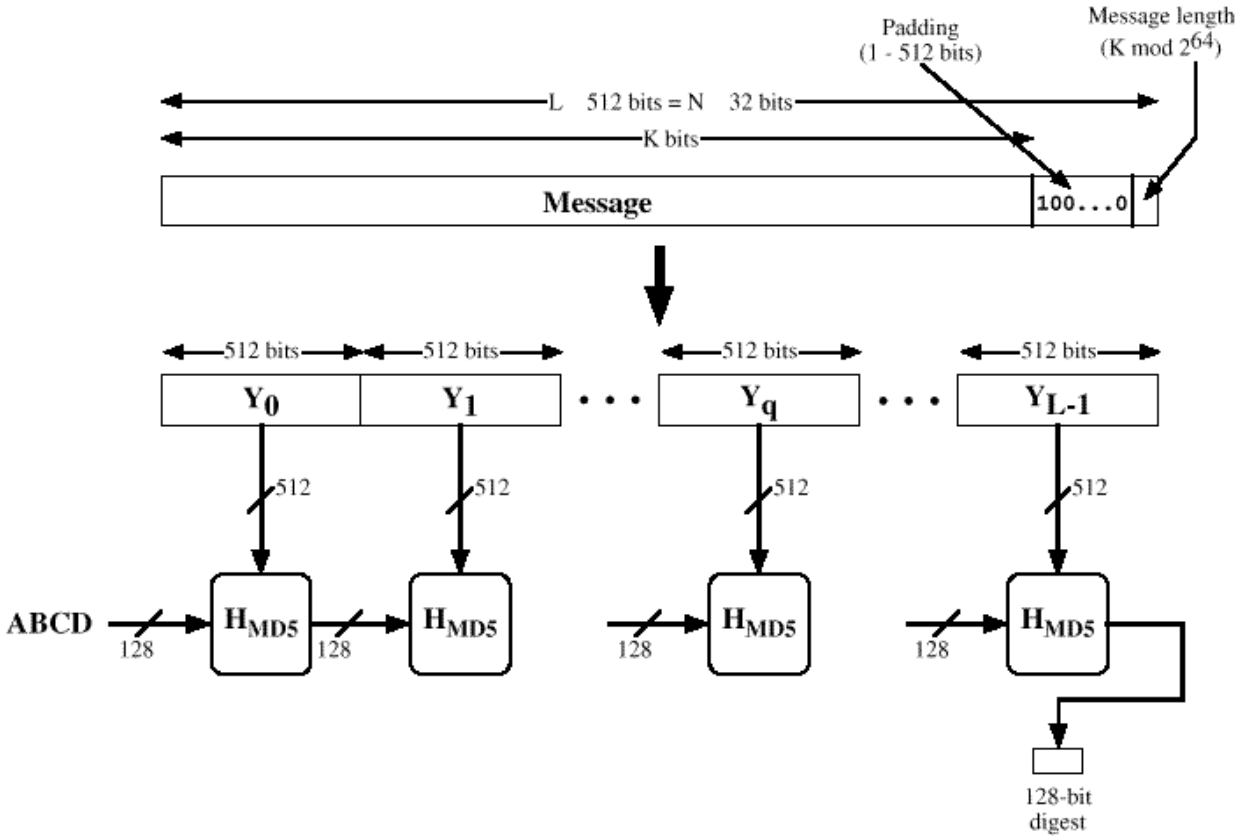


Figure 18.14 Message Digest Generation Using MD5

4. Public-key Encryption and Digital Signatures

- Public-key encryption
- The RSA public-key encryption algorithm
- Key management

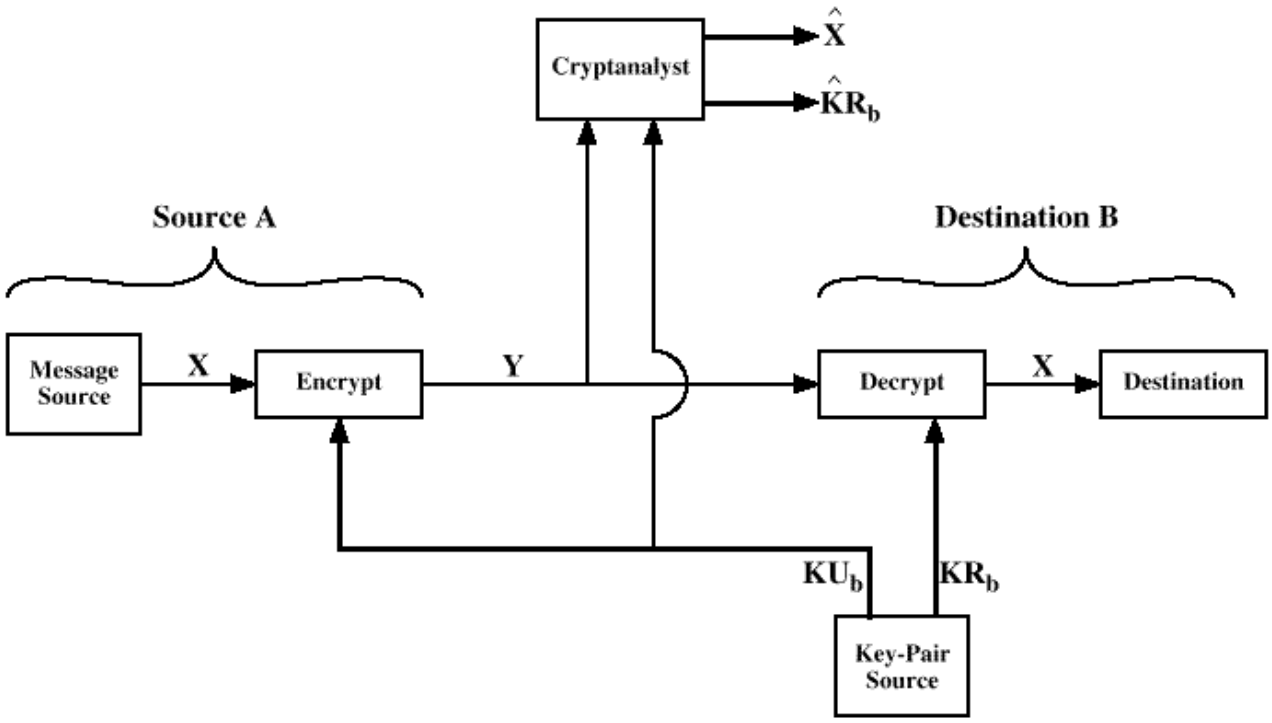


Figure 18.16 Public-Key Cryptosystem: Secrecy

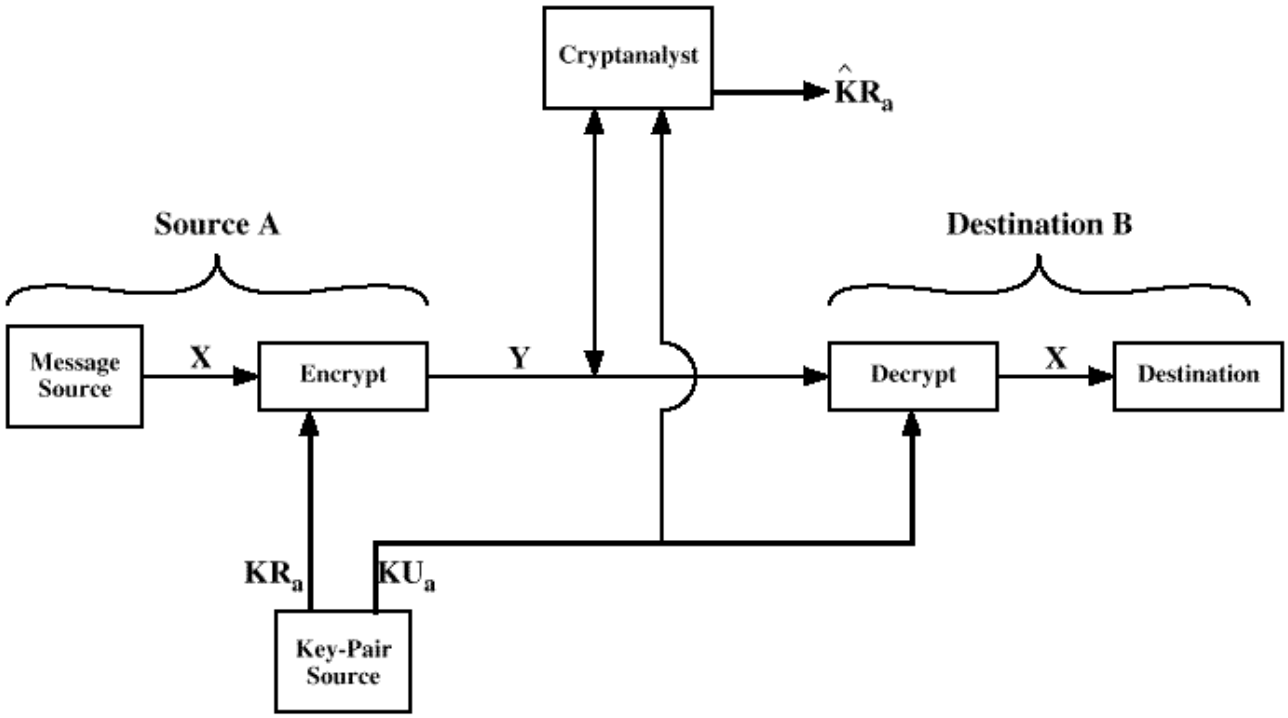
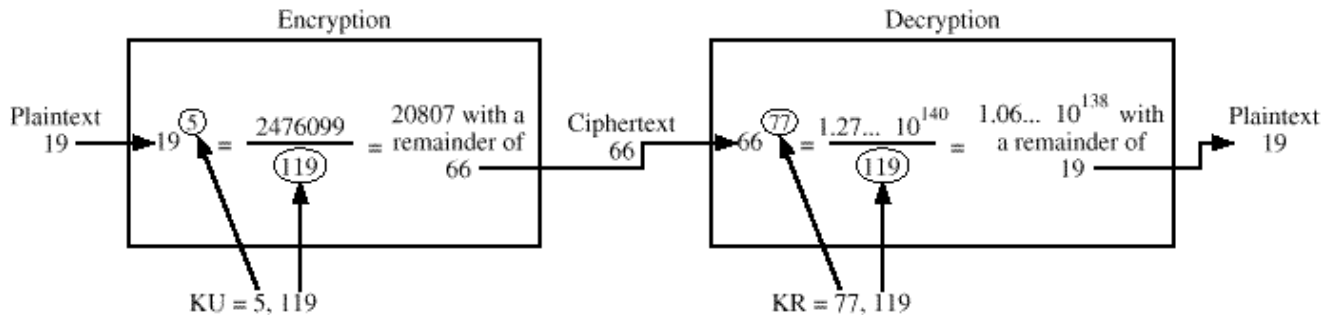


Figure 18.17 Public-Key Cryptosystem: Authentication


Encryption
Decryption
Plaintext
19
19^5 = 2476099 / 119 = 20807 with a remainder of 66
Ciphertext
66
66^77 = 1.27... 10^140 / 119 = 1.06... 10^138 with a remainder of 19
Plaintext
19
KU = 5, 119
KR = 77, 119

5. IPv4 and IPv6 Security

- Five security-related proposed standard
  - RFC 1825: An overview of a security architecture
  - RFC 1826: Description of a packet authentication extension to IP
  - RFC 1828: a specific authentication mechanism
  - RFC 1827: description of a packet encryption extension to IP
  - RFC 1829: a specific encryption mechanism
- extension header
  - authentication header
  - ESP(Encapsulating Security Payload) header

  - Security associations
    - IP address, SPI(security parameter index)
    - parameters
      - authentication algorithm/mode/key
      - encryption algorithm/mode/key
      - presence/absence/size of al cryptographic synchronization or initialization vector field for the encryption algorithm
      - etc.
- Authentication
    - provides
      - data integrity
      - IP packet authentication

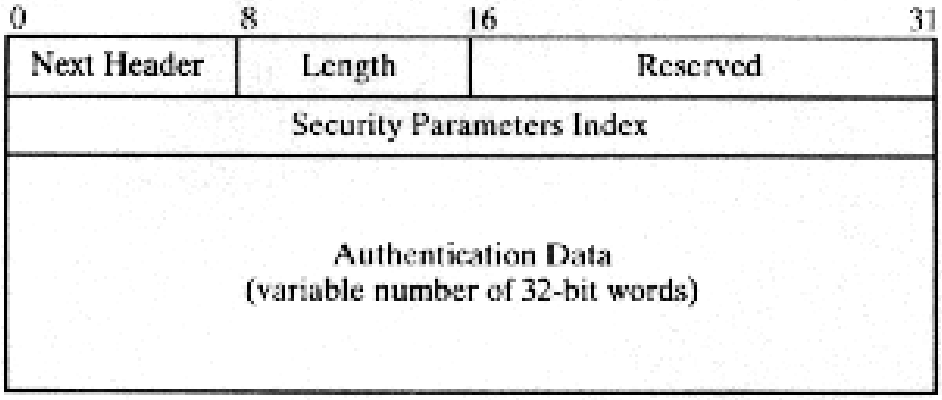


FIGURE 18.20 Authentication header.

- Authentication using keyed MD5
  - RFC 1828 specifies the use of MD5 for authentication
  - MD5 is performed over the IP packet plus a secret key
  - two types of authentication
    - end-to-end authentication
    - end-to-intermediate authentication

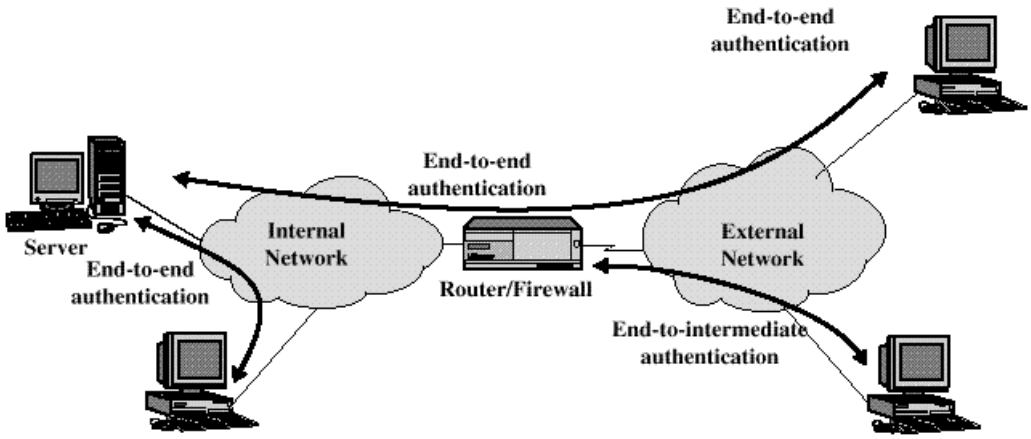
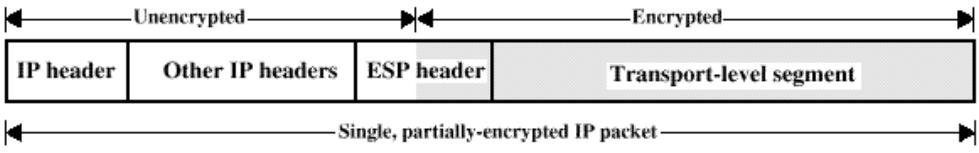
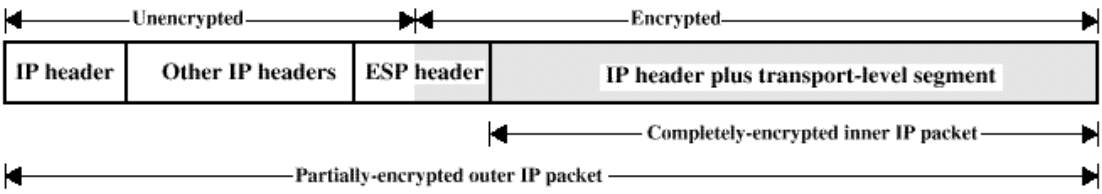


Figure 18.21 End-to-end vs. End-to-intermediate Authentication [DOTY95]

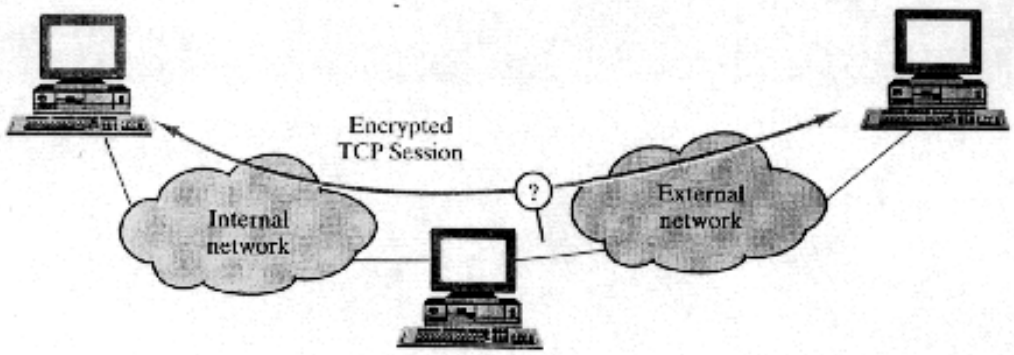
- Encapsulating security payload
  - provides
    - privacy
    - data integrity
  - transport-mode ESP
    - to encrypt the data carried by IP
      - transport-layer segment
    - procedure(fig18.22)
    - avoid the need to implement privacy in every individual application
    - vulnerable to traffic analysis
  - tunnel-mode ESP
    - encrypt an entire IP packet
    - procedure(fig18.22)
    - useful in a configuration that includes a firewall or other sort of security gateway



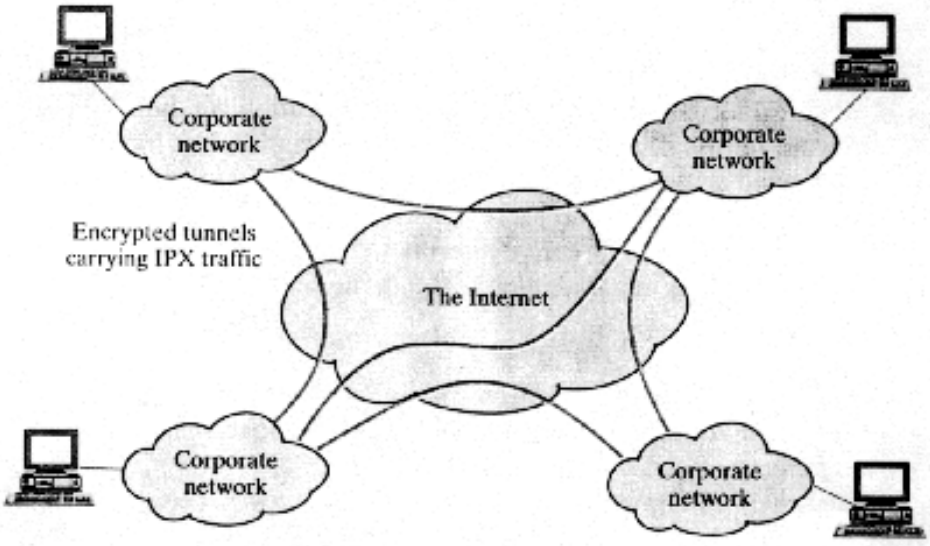
(a) Transport mode



(b) Tunnel mode



(a) Transport-level security



(b) A virtual private network via tunnel mode

FIGURE 18.23 Applications of encapsulating security payload [DOTY95].

– the ESP DES-CBC transform(fig18.24)

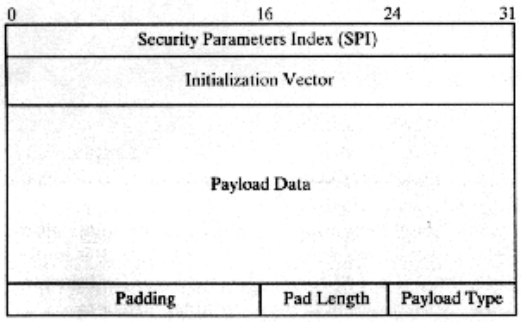
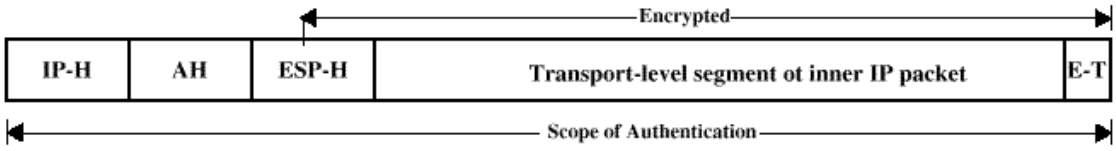
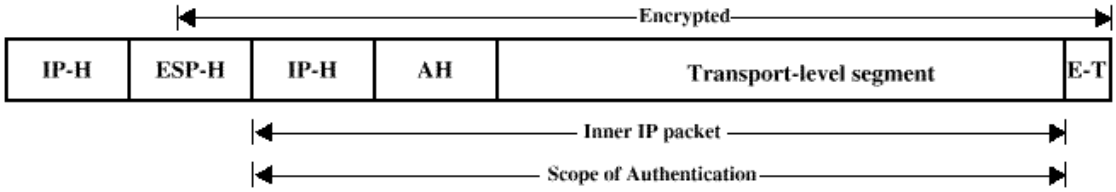


FIGURE 18.24 Encapsulating security payload format.

- Authentication plus privacy
  - encryption before authentication
  - authentication before ecnryption



(a) Encryption before authentication (transport or tunnel mode)



(b) Authentication before encryption (tunnel mode)

IP-H = IP base header plus extentions headers
ESP-H = Encapsulating Security Payload header
E-T = Encapsulating Security Payload trailing fields
AH = Authentication header

Figure 18.25 Combining Privacy and Authentication