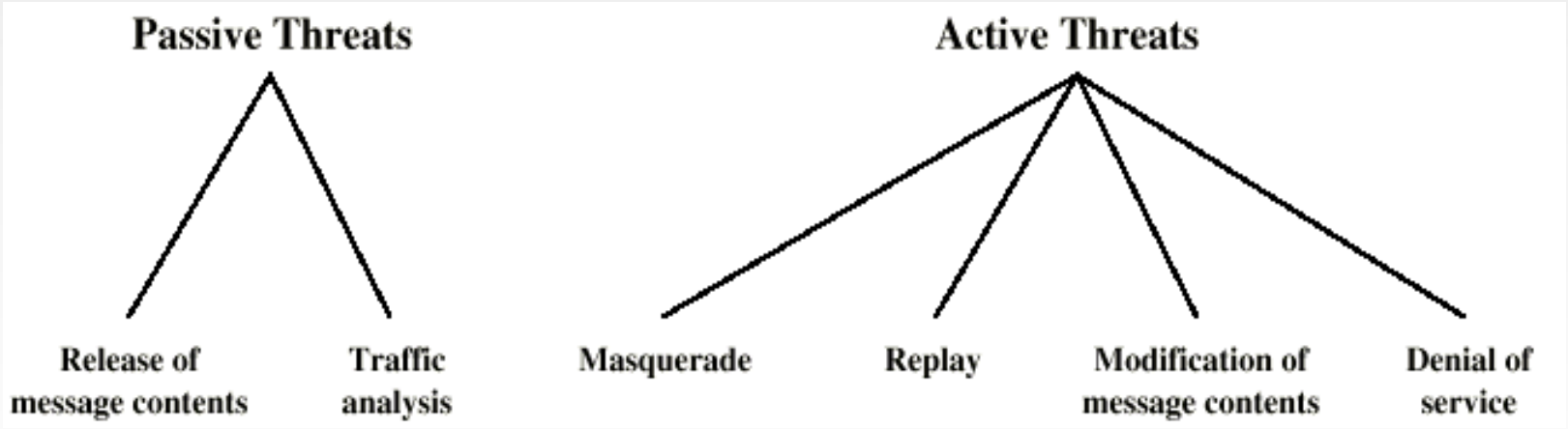
Network Security

Security Requirements:

- Confidentiality
- Integrity
- Availability

- Two types of attacks on network security:
  - Passive
  - Active

Security Threats:



Passive Attacks:

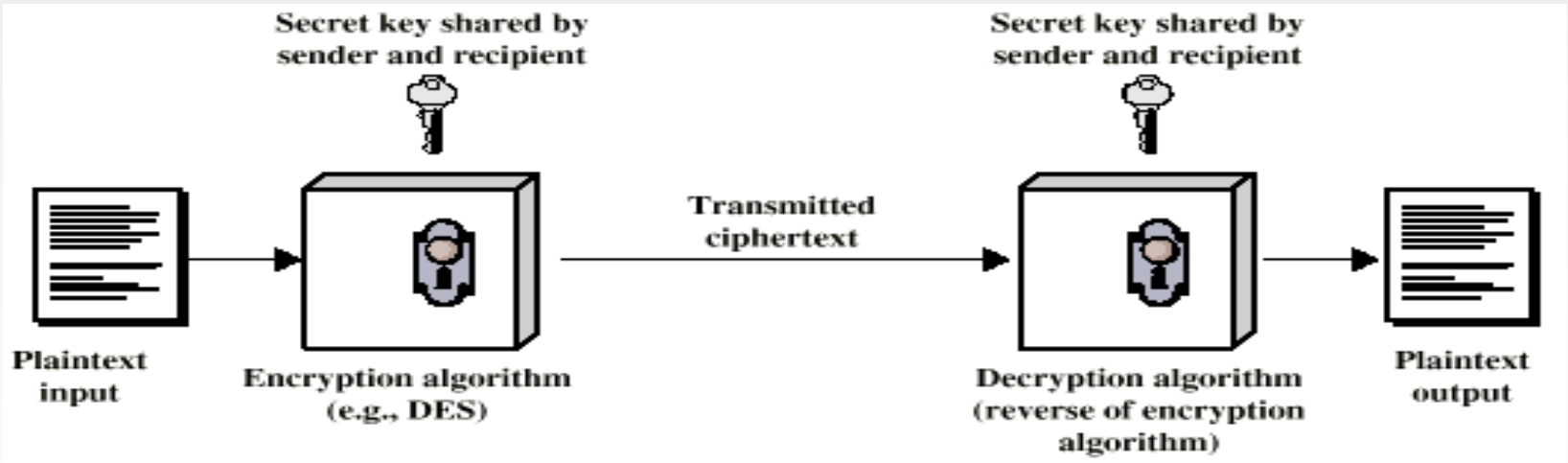
- Eavesdropping on transmissions to obtain information
- Two Types:
  - **Release of message contents:**
    - Outsider learns content of transmission
  - **Traffic analysis:**
    - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- Difficult to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

Active Attacks:

- **Masquerade**
  - Pretending to be a different entity
  - It includes one of the other types of active attack
  - e.g. Capture authentication sequence and replay after valid authentication to get extra privileges
- **Replay:**
  - Capture of data units and retransmission
- **Modification of messages:**
  - Modify/delay/reordered the message
- **Denial of service:**
  - Block the services/slow down the access/overloading the network by sending with other messages
- **Easy to detect**
  - Detection may lead to deterrent

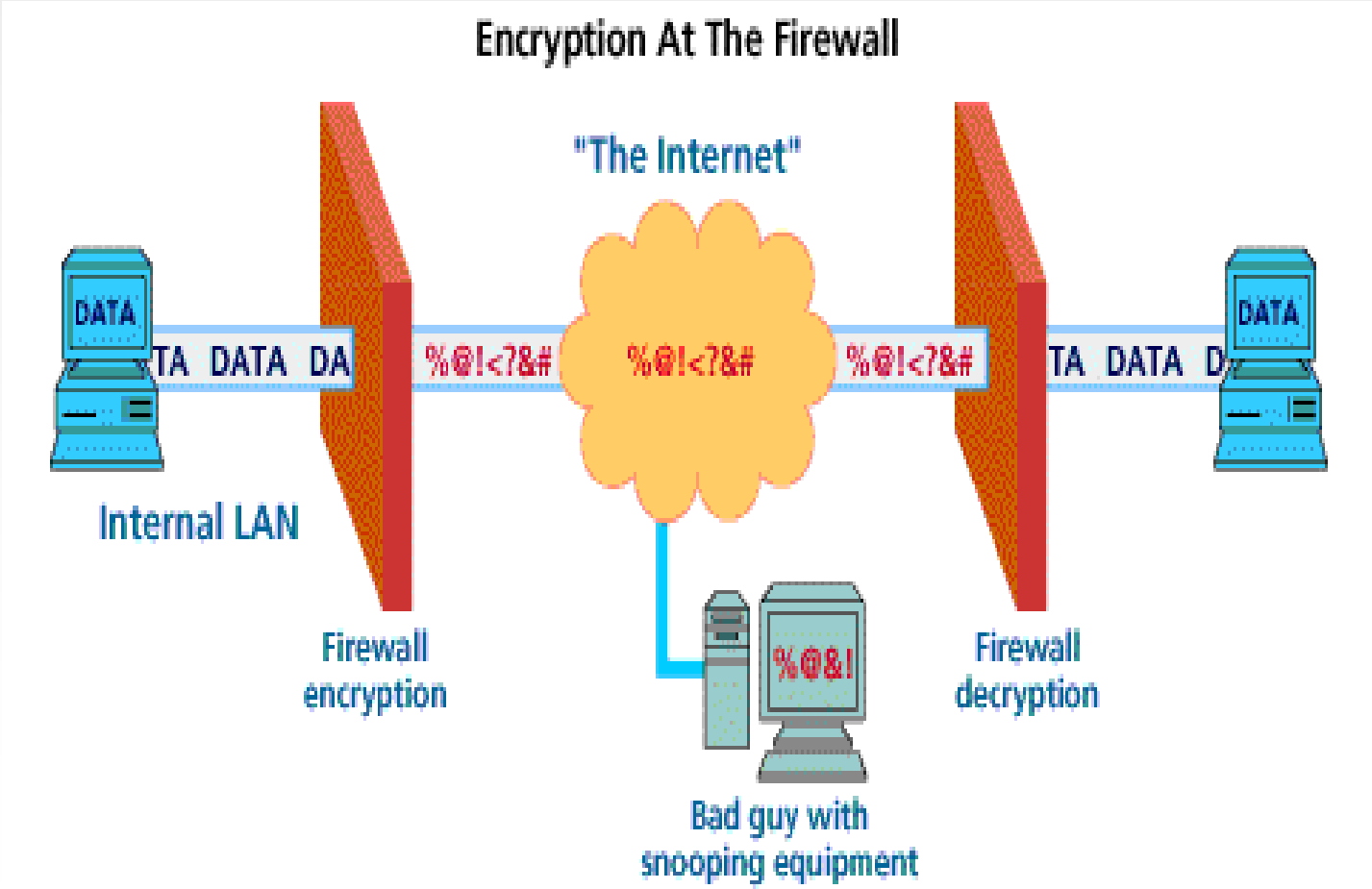
Conventional Encryption:

- **Symmetric/single-key encryption:**



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

Conventional Encryption:



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 a Conventional Encryption:

Two Approaches:

- Cryptanalysis:
  - Rely on nature of algorithm plus some knowledge of general characteristics of plain text/cipher text
  - Attempt to deduce plain text or key
- Brute force
  - Try every possible key until plain text is achieved
  - On average, half of all possible keys must be tried to get success

Attacking a Conventional Encryption:

- Average time required for exhaustive key search:

Key size (bits)	Number of alternative keys	Time required at 1 decryption/ µs	Time required at 10^6 decryption/ µs
32	$2^{32} = 4.3 \times 10^9$	2^{31}µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55}µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127}µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167}µs = 5.9×10^{36} years	5.9×10^{30} years

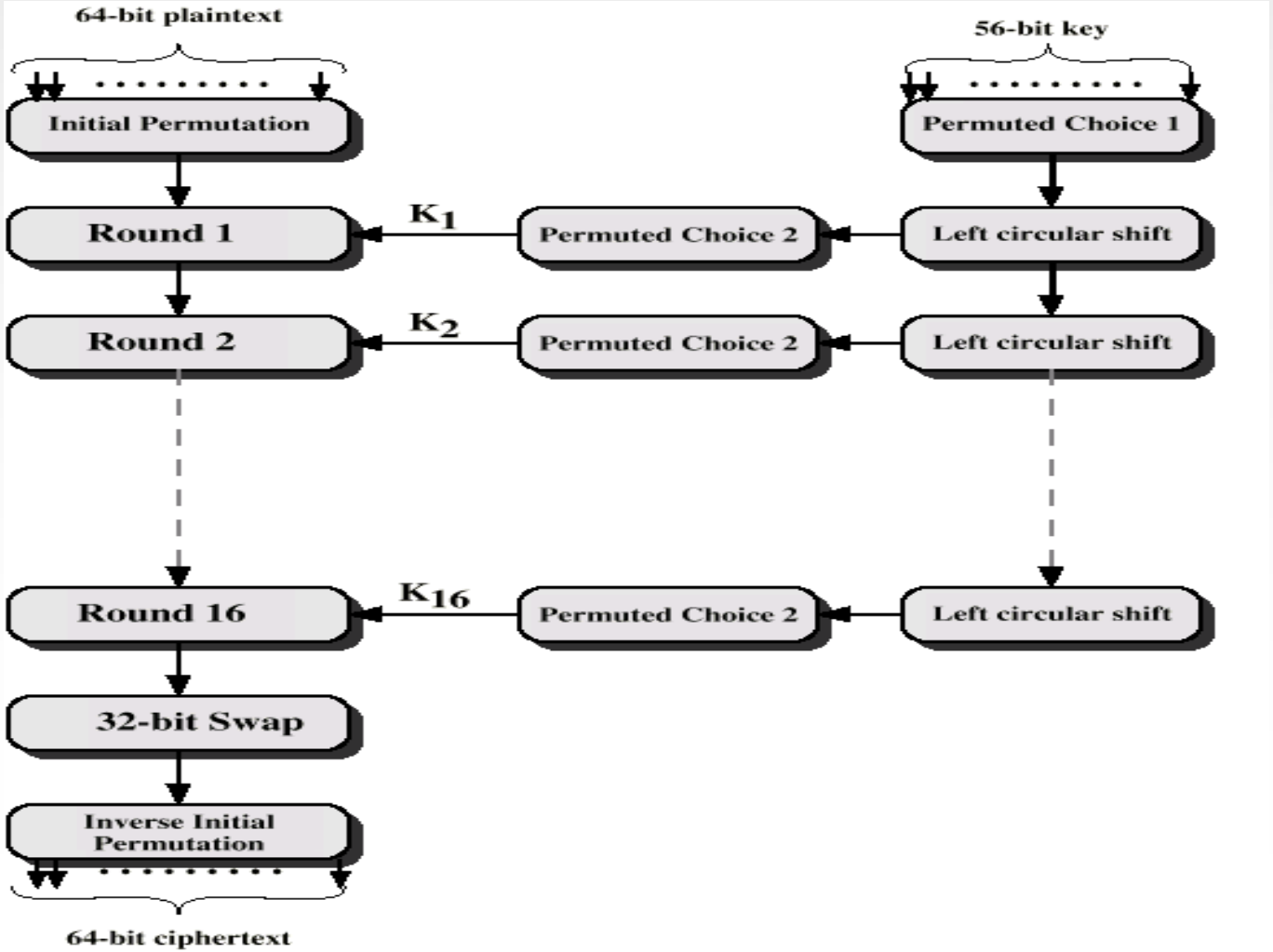
Algorithms:

- Most commonly used conventional algorithms are block ciphers:
  - **Process plain text in fixed block sizes producing block of cipher text of equal size**
    - **Data encryption standard (DES)**
    - **Triple DES (TDES)**
    - **Advanced DES**

Data Encryption Standard (DES):

- Data Encryption Algorithm
- Adopted by ANSI
- 64 bit plain text blocks
- 56 bit key

DES Encryption Algorithm:



DES Encryption Algorithm:

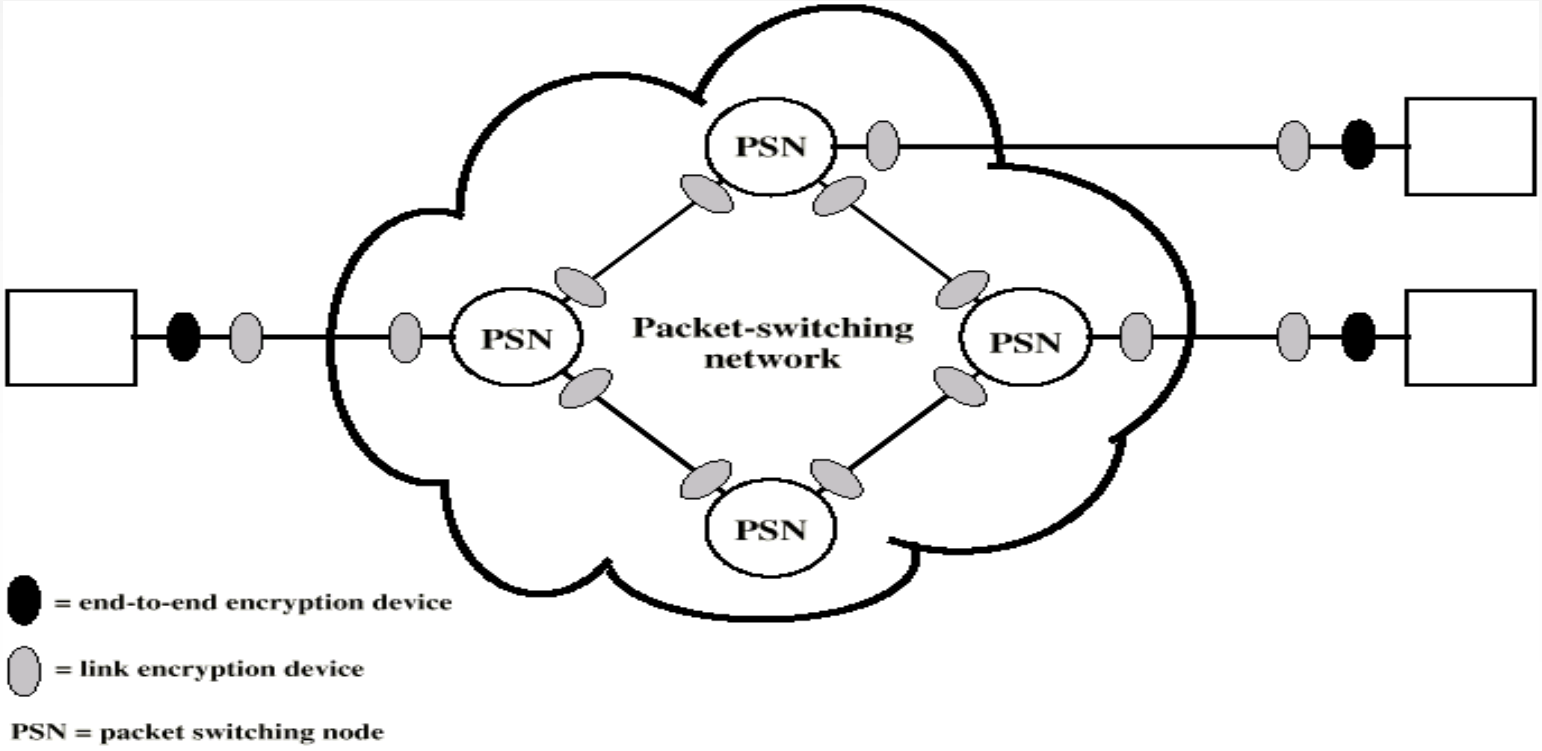
- Declared insecure in 1998
- Alternatives include TDES/ADES
- Advanced Encryption Algorithm:
  - **RSA Encryption**
  - **Twofish encryption algorithm**
  - **Blowfish encryption algorithm**
  - **IDEA encryption algorithm**
  - **MD5 encryption algorithm**
  - **HMAC encryption algorithm**

Triple Data Encryption Algorithm:

- 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:

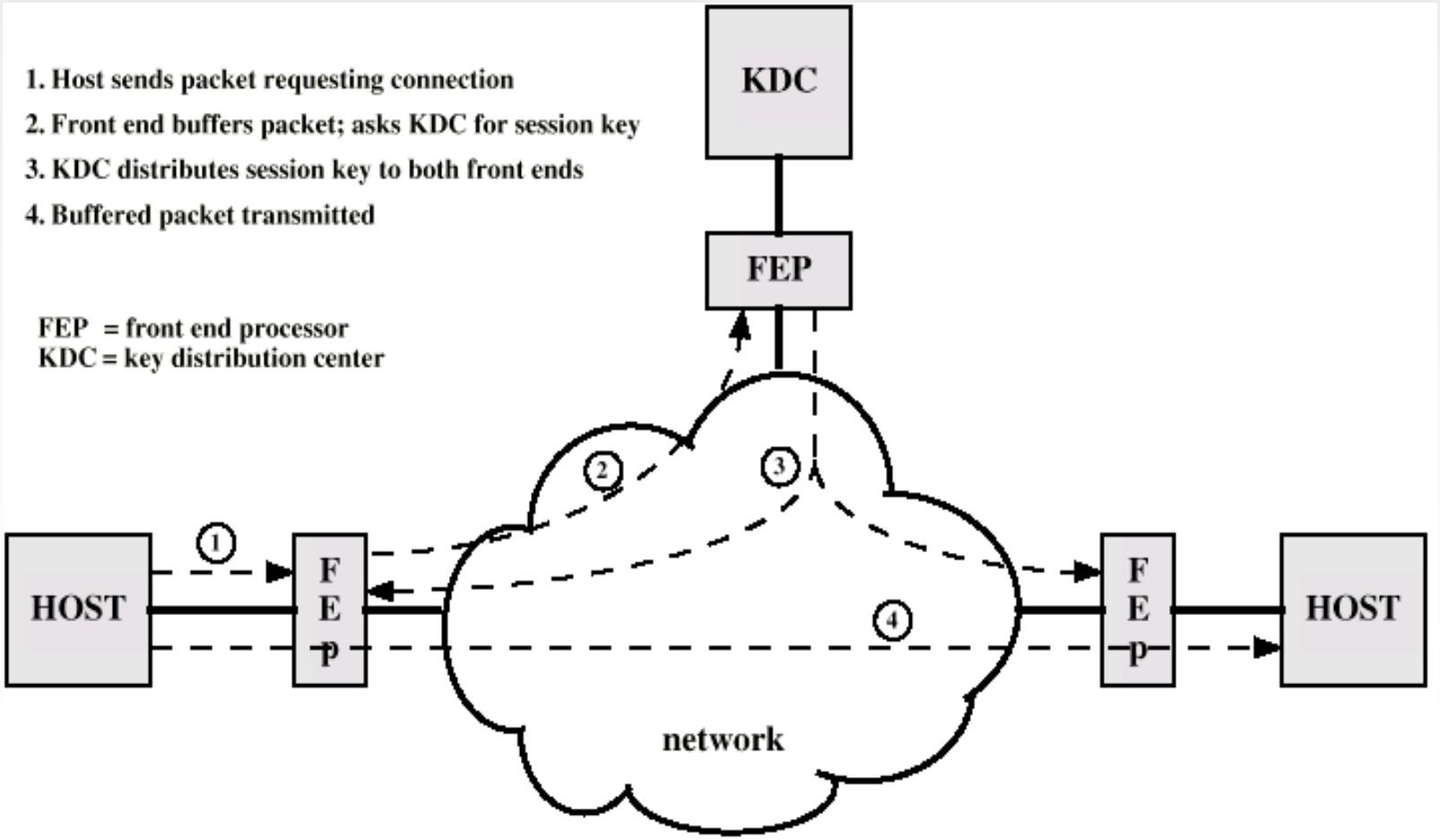
- Two fundamental alternatives:
  - link encryption
  - end to end encryption



Key Distribution:

- Key could be selected by A and physically delivered to B
- Third party could select key and physically deliver 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 for connection oriented protocol:



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 passive attacks:
  - Encryption
- Protection against active attacks:
  - Falsification of data/transactions
  - Authentication
- Message is authentic if it is genuine and comes from the real source
- Authentication allows receiver to verify that message is authentic
  - Message has not altered
  - Message is from authentic source
  - Message timeliness

Authentication Using Encryption

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

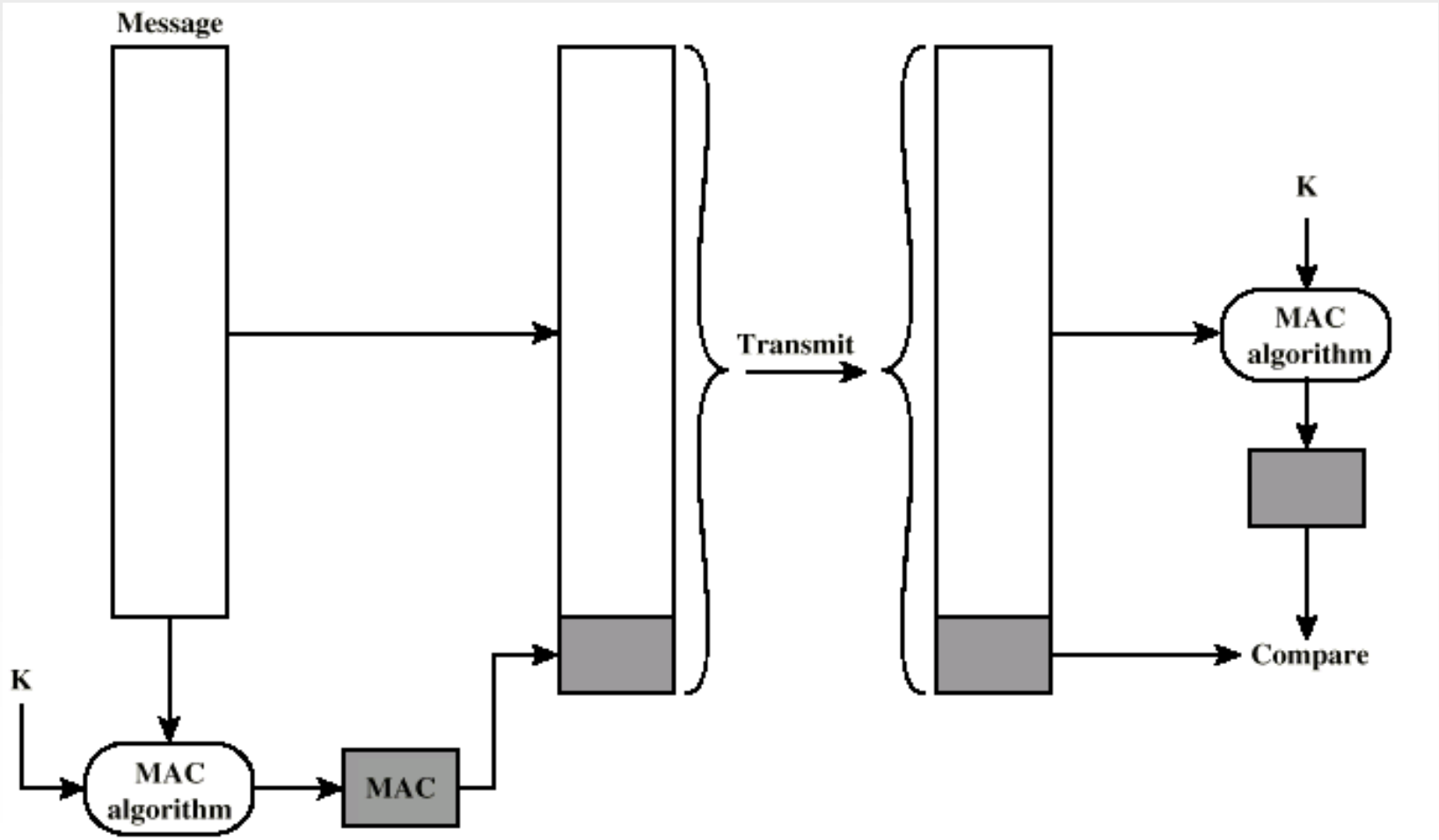
Authentication Without Encryption

- 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

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 if 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

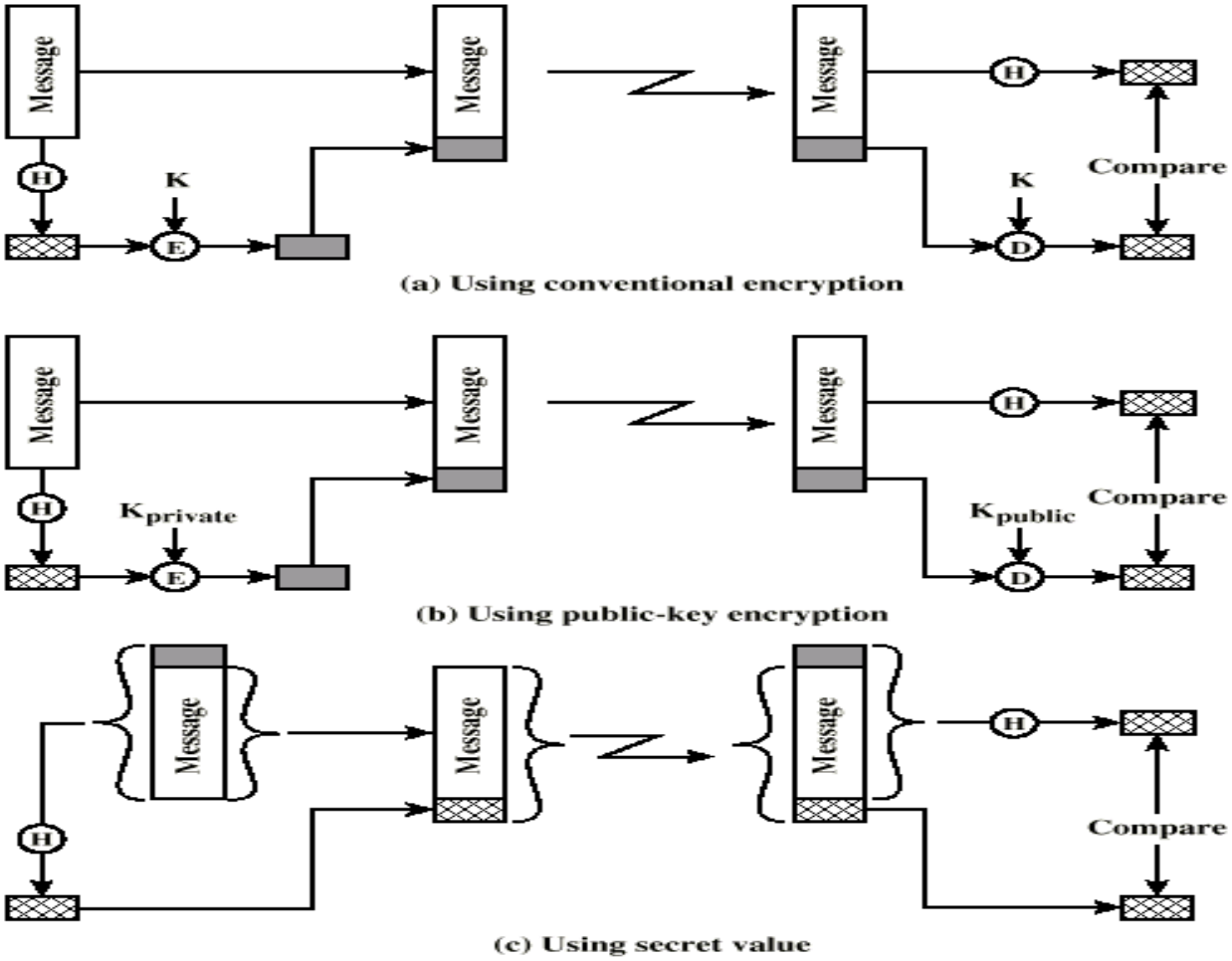
Message Authentication Using Message Authentication Code



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

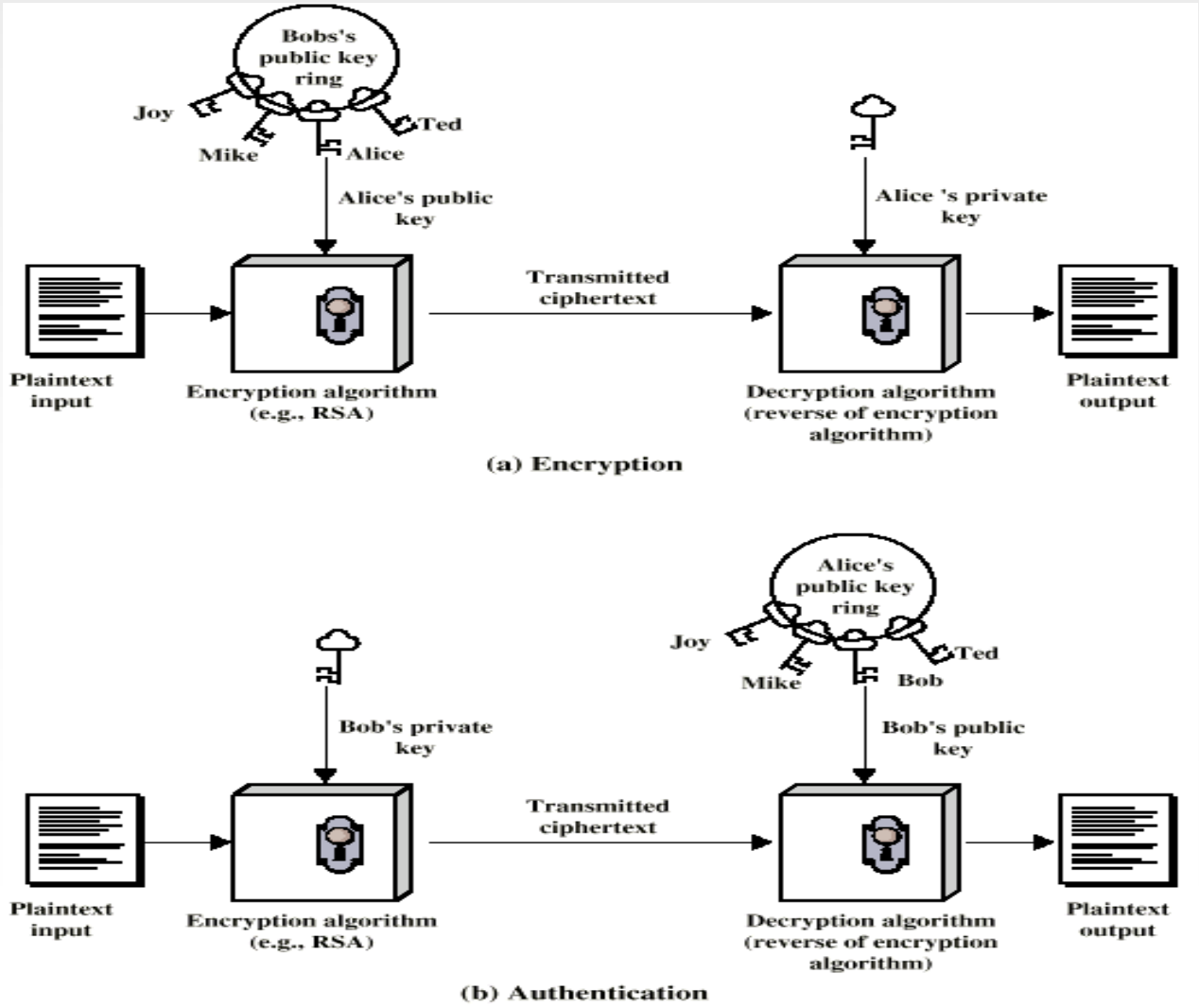
Using One Way Hash:



Public Key Encryption:

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

Public Key Encryption:



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 senders public key
- This authenticates sender, who is only person who has the matching key
- Does not give privacy of data
  - Decrypt key is public