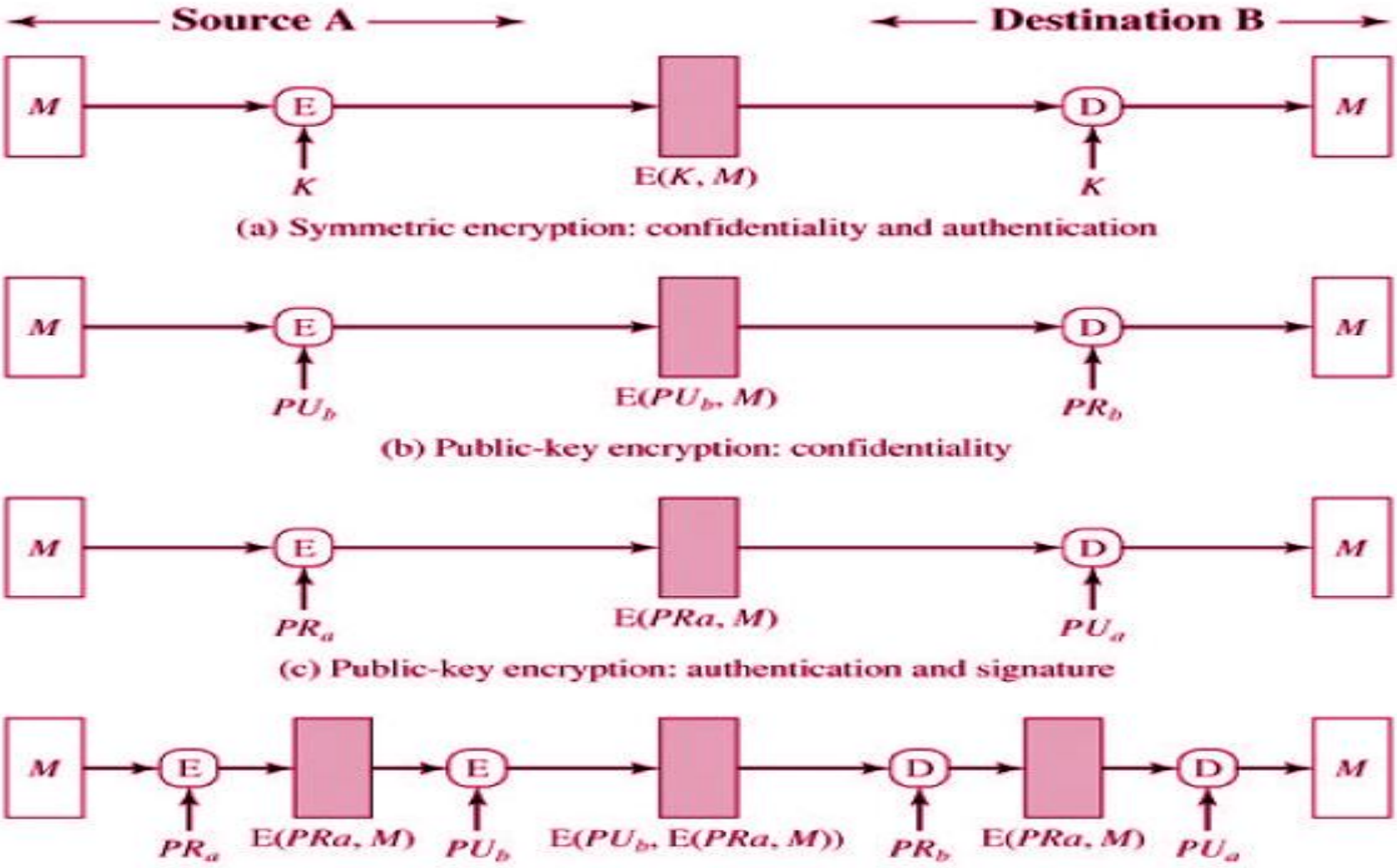
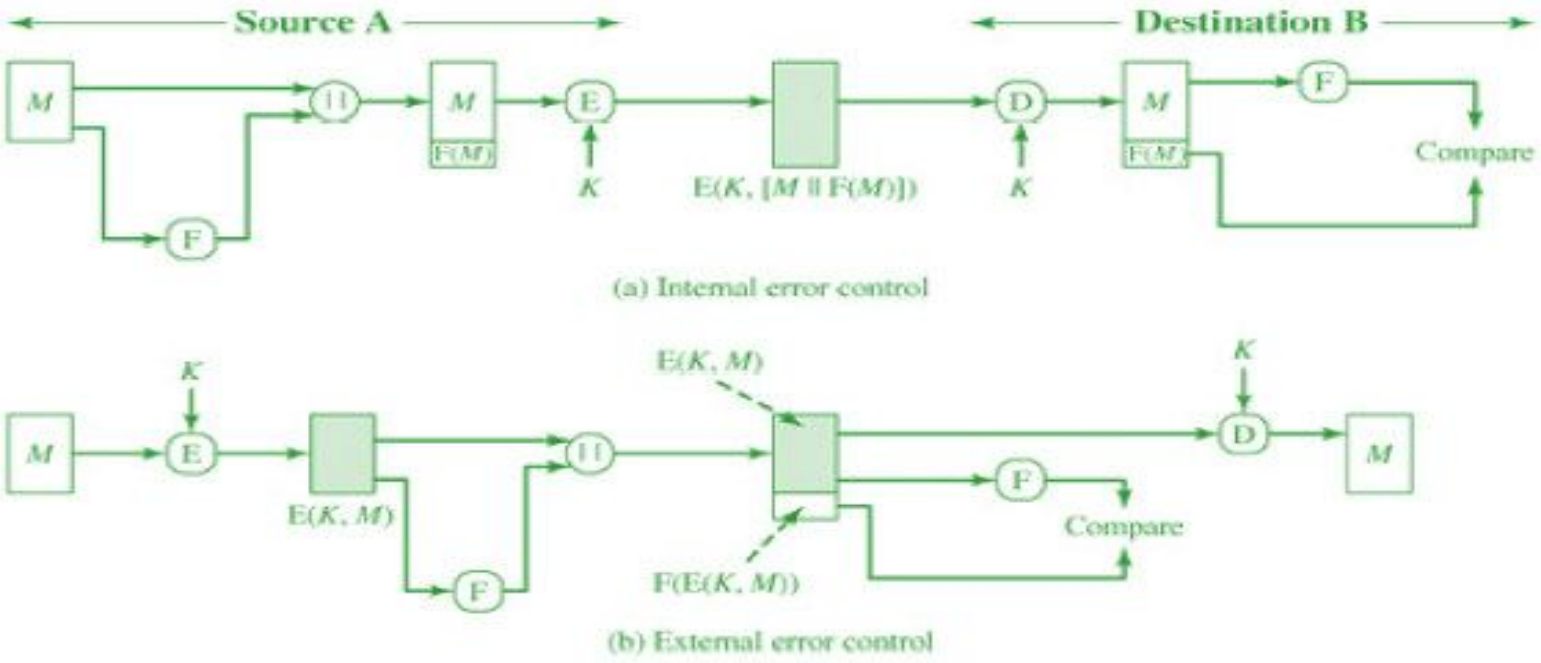
# MESSAGE AUTHENTICATION CODE AND HASH FUNCTIONS

- For a secure communication
  - Authentication
  - Confidentiality
  - Integrity
  - Non repudiation

# Symmetric Encryption

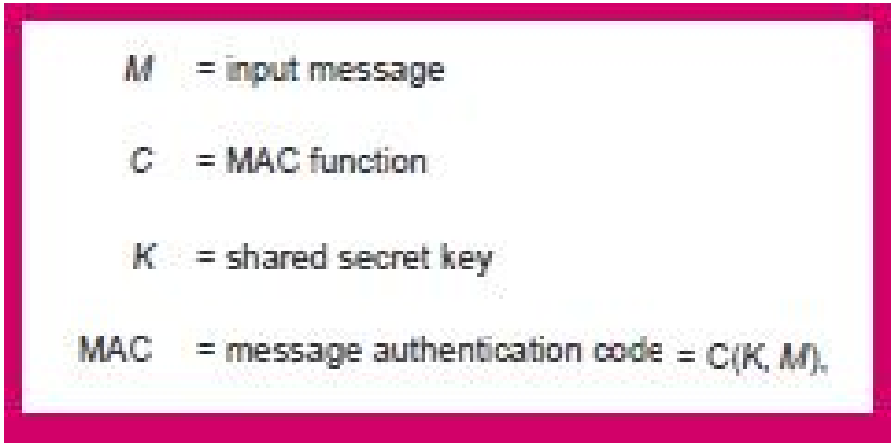


- None of the above system provides data integrity aka message authentication.
- Solution to problem : USING CHECKSUM (FCS)

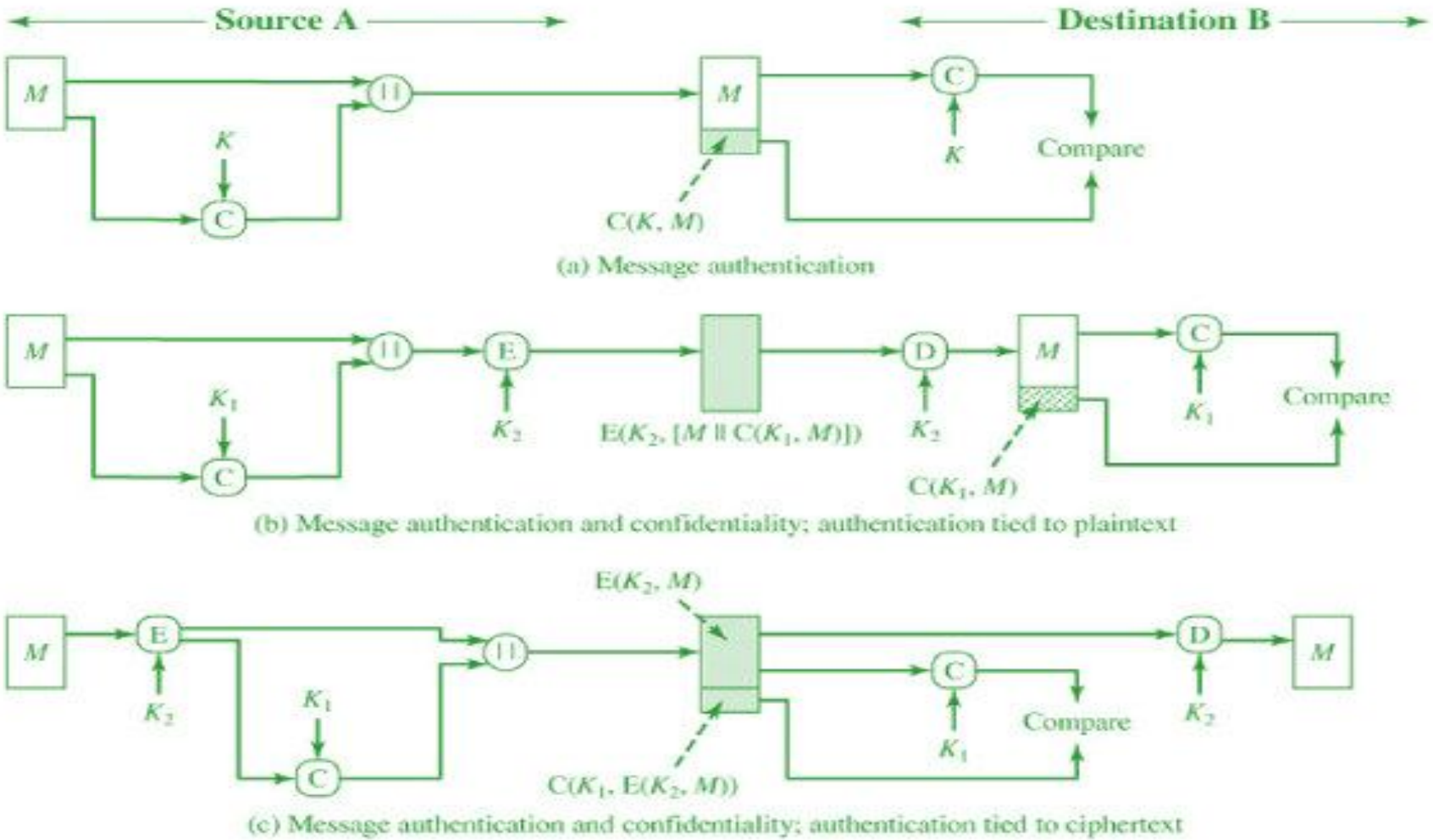


# MAC

- Another solution is message authentication code knows as cryptographic checksum
  - Involves using a second key.



# MAC cont'd


Source A
Destination B
M
K
C
||
M
C(K, M)
K
Compare
(a) Message authentication
M
K1
C
||
E
K2
E(K2, [M || C(K1, M)])
D
K2
M
C(K1, M)
C
K1
Compare
(b) Message authentication and confidentiality; authentication tied to plaintext
M
E
K2
K1
C
||
E(K2, M)
C(K1, E(K2, M))
C
K1
Compare
D
K2
M
(c) Message authentication and confidentiality; authentication tied to ciphertext

# MAC cont'd

- Similar to encryption function
  - Only non reversible.
- It is many-to-one function.
  - If an $n$-bit MAC is used, then there are $2^n$ possible MACs, whereas there are N possible messages with $N >> 2^n$. Furthermore, with a $k$-bit key, there are $2^K$ possible keys.

For example, suppose that we are using 100-bit messages and a 10-bit MAC. Then, there are a total of $2^{100}$ different messages but only$2^{10}$ different MACs. So, on average, each MAC value is generated by a total of $2^{100}$ /$2^{10}$= $2^{90}$ different messages. If a 5-bit key is used, then there are 2 5= 32 different mappings from the set of messages to the set of MAC values.

- It turns out that because of the mathematical properties of the authentication function, it is less vulnerable to being broken than encryption.

# HASH FUNCTION

- A Hash Function is a well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data "m" into a small datum called HashValue defined by h:=h(m)

- IV is the initial value given as input to the hash function [Initial/Group key]

# HASH FUNCTIONS

- The Cryptographic hash function has Some significant properties :
  - The input can be of a variable length while The output has a fixed length
  - Easy to compute the hash value for any given message.
  - The description of h must be publicly known and should not require any secret information for its operation
  - **One Way Function** : it is infeasible to extract a message from its given hash.
  - It is infeasible to modify a message without changing its hash .
  - **Collision Resistant** :There are NO two different distinct messages with the same hash result .

- There are a series of well know hash functions . Most commonly used in Cryptography is MD "Message Digest Algorithm" [MD4, MD5, MD6, RIPE-MD ]And the SHA "Secure Hash Algorithm" series (1,224, 256, 384, 512)

| | SHA-1 | SHA-256 | SHA-384 | SHA-512 |
|---|---|---|---|---|
| Message digest size | 160 | 256 | 384 | 512 |
| Message size | $<2^{64}$ | $<2^{64}$ | $<2^{128}$ | $<2^{128}$ |
| Block size | 512 | 512 | 1024 | 1024 |
| Word size | 32 | 32 | 64 | 64 |
| Number of steps | 80 | 64 | 80 | 80 |
| Security | 80 | 128 | 192 | 256 |