Lecture-8

Eng. Taghreed Harfoush

INFORMATION SECURITY

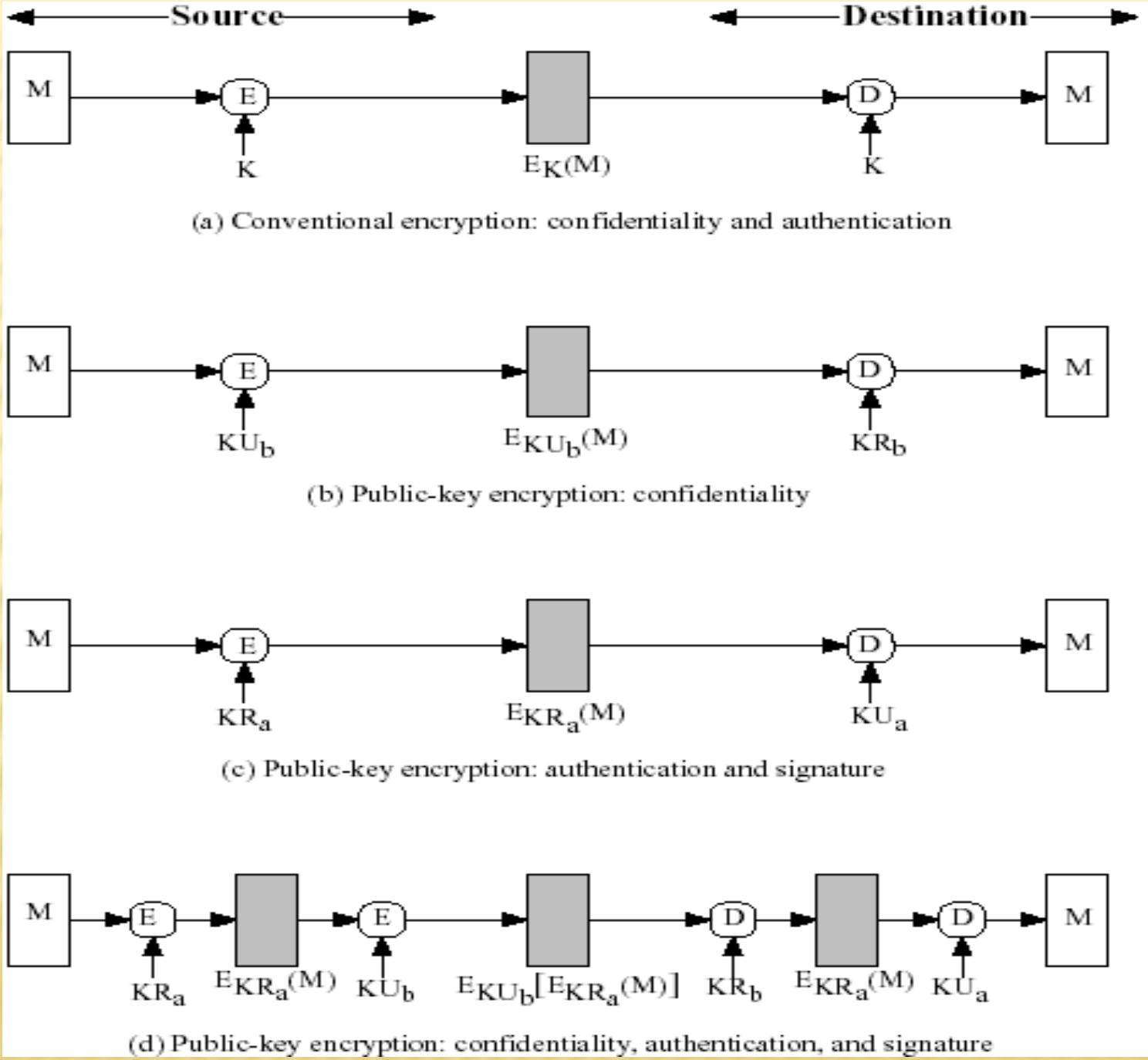
AUTHENTICATION FUNCTIONS

- Message authentication or digital signature mechanism can be viewed as having two levels
  - At lower level: there must be some sort of functions producing an authenticator – a value to be used to authenticate a message
    - Message encryption
    - Hash function
    - Message authentication code (MAC)
  - This lower level functions is used as primitive in a higher level authentication protocol

- Message encryption
  - Ciphertext itself serves as authenticator
- Message authentication code (MAC)
  - A public function of the message and a secret key that produces a fixed-length value that serves as the authenticator
- Hash function
  - A public function that maps a message of any length into a fixed-length hash value, which serves as the authenticator

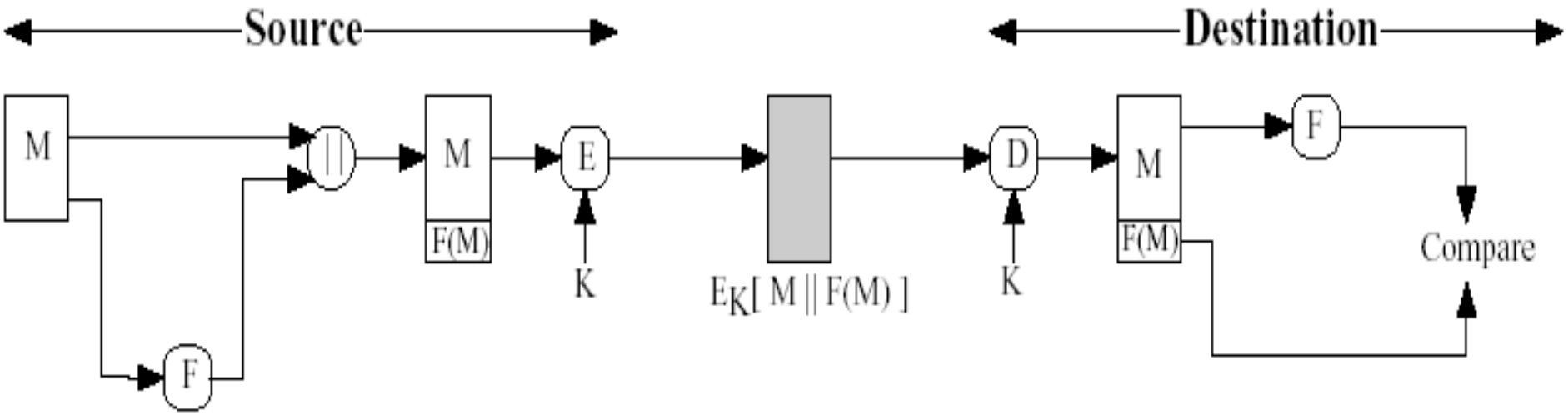
BASIC USES OF MESSAGE ENCRYPTION

- Conventional encryption can serve as authenticator
  - Conventional encryption provides authentication as well as confidentiality
  - Requires recognizable plaintext or other structure to distinguish between well-formed plaintext and meaningless random bits
    - e.g., ASCII text, an appended checksum, or use of layered protocols
- Public key encryption
  - Provide Authentication via the use of private key.

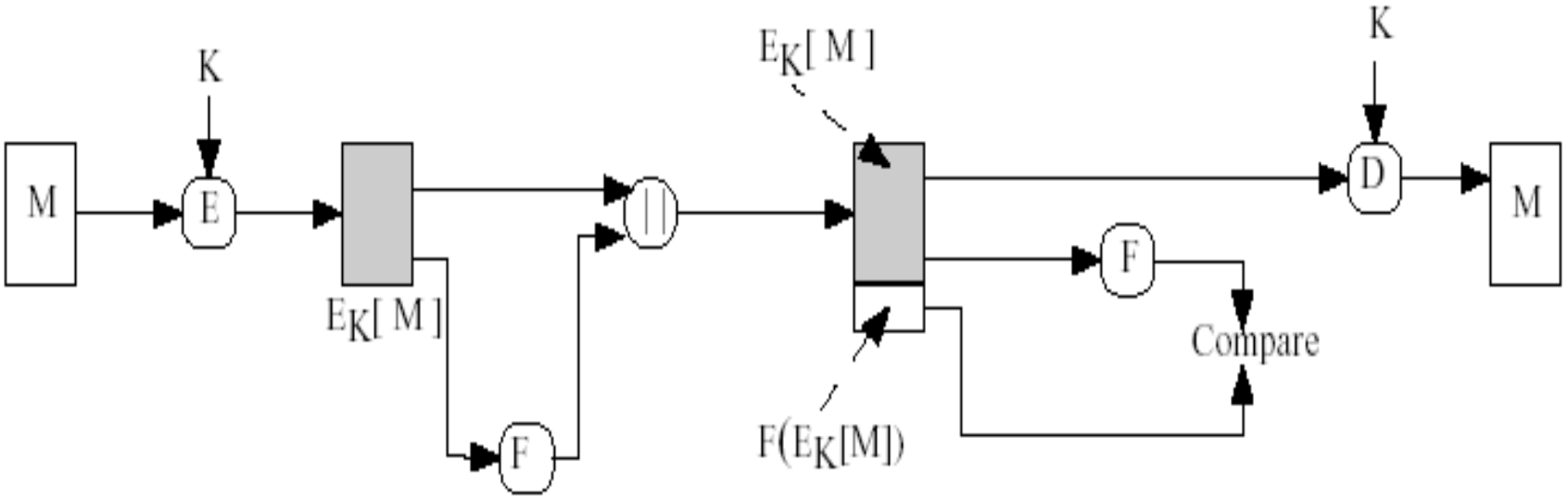

Source
Destination
M
E
K
$E_K(M)$
D
K
M
(a) Conventional encryption: confidentiality and authentication
M
E
KU_b
$E_{KU_b}(M)$
D
KR_b
M
(b) Public-key encryption: confidentiality
M
E
KR_a
$E_{KR_a}(M)$
D
KU_a
M
(c) Public-key encryption: authentication and signature
M
E
KR_a
$E_{KR_a}(M)$
E
KU_b
$E_{KU_b}[E_{KR_a}(M)]$
D
KR_b
$E_{KR_a}(M)$
D
KU_a
M
(d) Public-key encryption: confidentiality, authentication, and signature

WAYS OF PROVIDING STRUCTURE

- Append an error-detecting code (frame check sequence (FCS)) to each message



(a) Internal error control



(b) External error control

Confidentiality and Authentication Implications of Message Encryption

(a) Conventional (symmetric) Encryption

$A \rightarrow B: E_K[M]$

- Provides confidentiality
  - —Only A and B share K
- Provides a degree of authentication
  - —Could come only from A
  - —Has not been altered in transit
  - —Requires some formatting/redundancy
- Does not provide signature
  - —Receiver could forge message
  - —Sender could deny message

(b) Public-Key (asymmetric) Encryption

$A \rightarrow B: E_{KU_b}[M]$

- Provides confidentiality
  - —Only B has KR_b to decrypt
- Provides no authentication
  - —Any party could use KU_b to encrypt message and claim to be A

$A \rightarrow B: E_{KR_a}[M]$

- Provides authentication and signature
  - —Only A has KR_a to encrypt
  - —Has not been altered in transit
  - —Requires some formatting/redundancy
  - —Any party can use KU_a to verify signature

$A \rightarrow B: E_{KUb}[E_{KRa}(M)]$

- Provides confidentiality because of KU_b
- Provides authentication and signature because of KR_a

Q&A