SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 5: CYBER SECURITY SAFEGUARDS AND SECURITY SERVICES

Topic : Cyber Security Safeguards

Message Authentication

- Message authentication is concerned with:
  - Protecting the integrity of a message
  - Validating identity of originator
  - Non-repudiation of origin (dispute resolution)
- Will consider the security requirements

Requirements

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Content modification
5. Sequence modification
6. Timing modification
7. Source repudiation
8. Destination repudiation

- Measures to deal with first two attacks:
  - In the realm of message *confidentiality*, and are addressed with *encryption*
- Measures to deal with items 3 through 6
  - Message *authentication*
- Measures to deal with items 7
  - *Digital signature*
- Measures to deal with items 8
  - *Digital signature and protocol to counter the attack*

Message Authentication and Digital Signature

- Message authentication
  - A procedure to verify that messages come from the alleged source and have not been altered
  - Message authentication may also verify sequencing and timeliness
- Digital signature
  - *An authentication technique* that also includes measures to counter repudiation by either source or destination

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
  - This lower level functions is used as primitive in a higher level authentication protocol

3 classes of function that produce an authenticator

Hash Function

A public function that maps a message of any length into a fixed-length hash value, which serves as the authenticator

Message Encryption

Ciphertext itself serves as authenticator

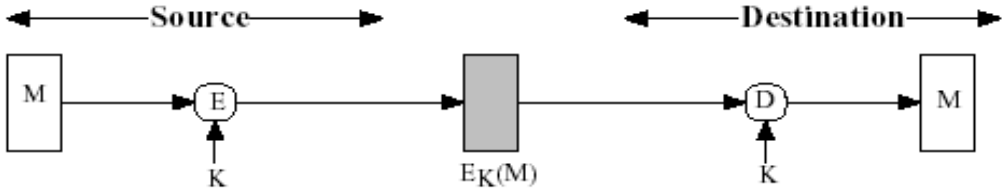
Message authentication code (MAC)

A public function of the message and a secret key that produces a fixed-length value that serves as the authenticator

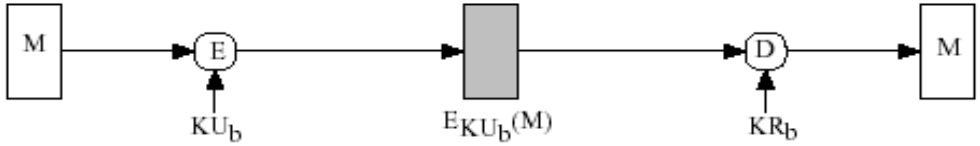
Message Encryption

- 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 legitimate plaintext and meaningless random bits
    - e.g., ASCII text, an appended checksum, or use of layered protocols

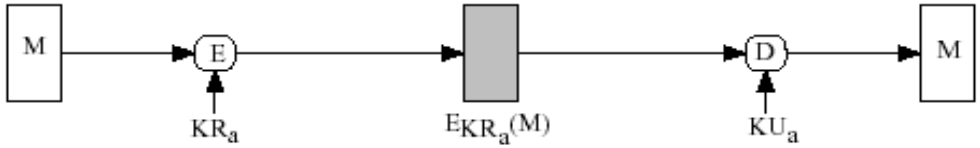
Basic Uses of Message Encryption



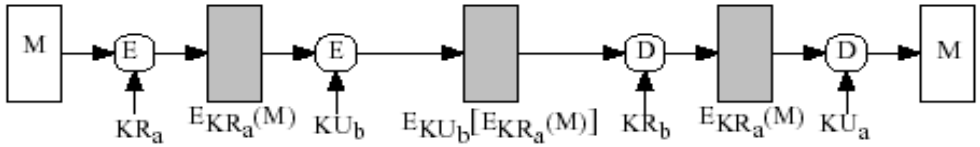
(a) Conventional encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality



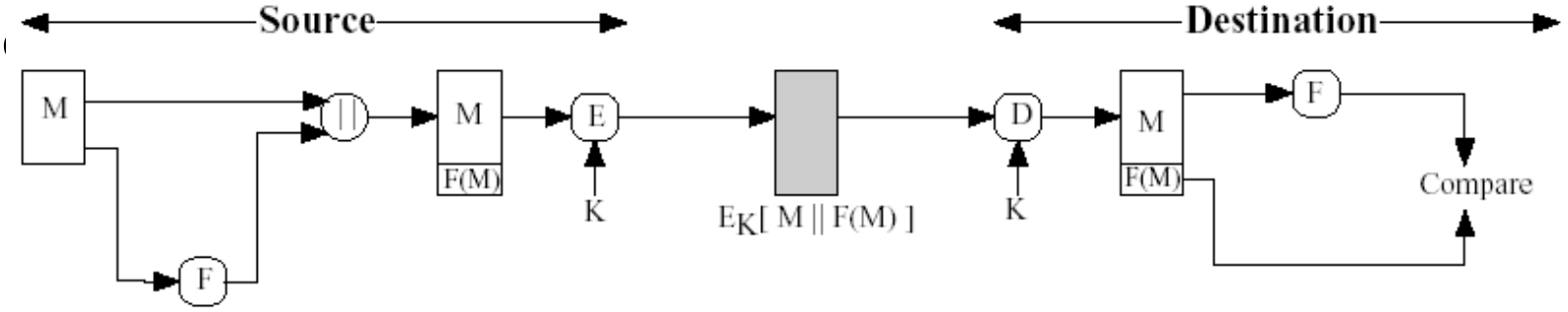
(c) Public-key encryption: authentication and signature



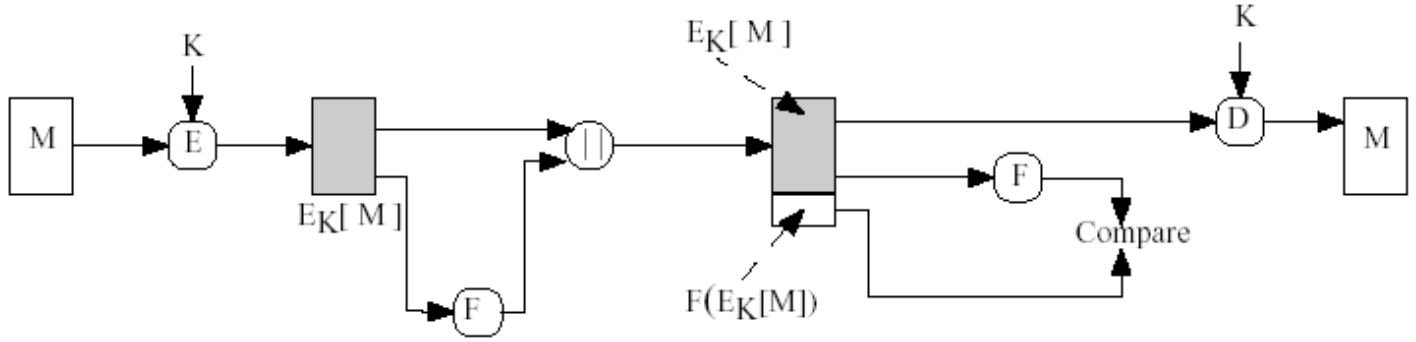
(d) Public-key encryption: confidentiality, authentication, and signature

Ways of Providing Structure

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



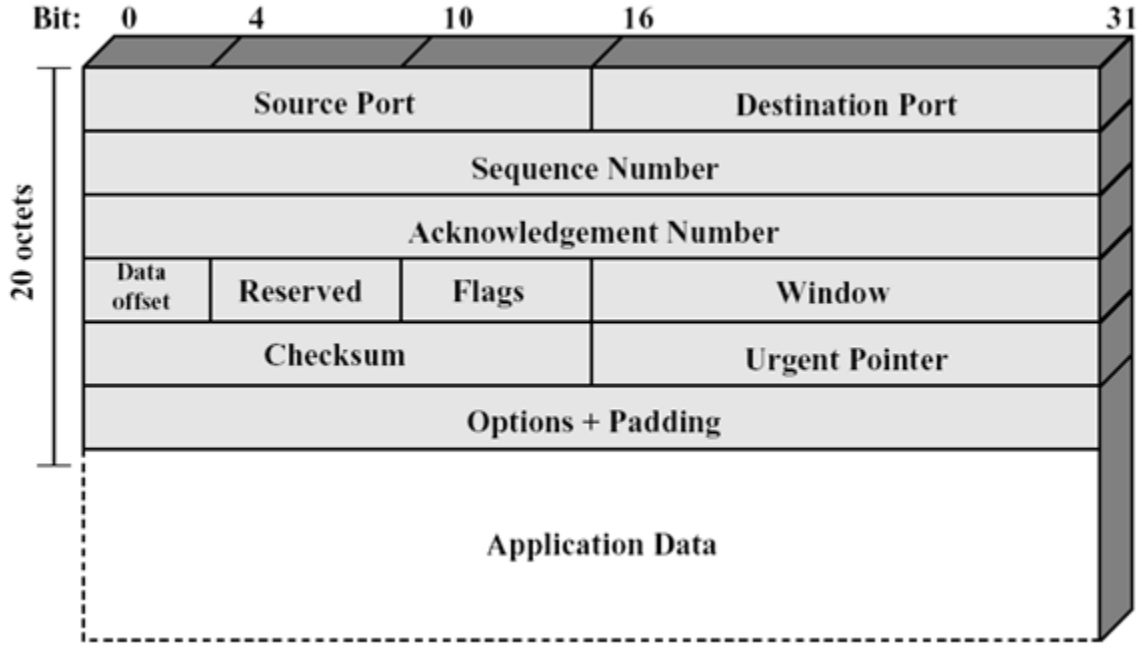
(a) Internal error control



(b) External error control

Ways of Providing Structure

- Suppose all the datagrams except the IP header is encrypted.
- If an opponent substituted some arbitrary bit pattern for the encrypted TCP segment, the resulting plaintext would not include



Confidentiality and Authentication

Impli

(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

Thank You