Material borrowed from slides available at http://williamstallings.com

Message Authentication

Presented by: Ruchika Mehresh

Center of Excellence in Information Systems Assurance Research and Education

University at Buffalo
The State University of New York

Shambhu J. Upadhyaya
Computer Science and Engineering
University At Buffalo,
Buffalo, New York , 14260

CSE565: Computer Security

Hash Function

- Hash function (H)
  - accepts a variable-length block of data (M) as input and produces a fixed-size hash value

$$\mathbf{h=H(M)}$$

- Good hash functions
  - evenly distributed
  - apparently random

Cryptographic Hash Functions

- Hash functions needed for security applications
- Computationally infeasible:
  - (given h) to find x s.t. H(x)=h
    - one-way property
  - (given x) to find y s.t. H(y)=H(x)
    - weak collision resistance
  - to find any x,y s.t. H(y)=H(x)
    - strong collision resistance

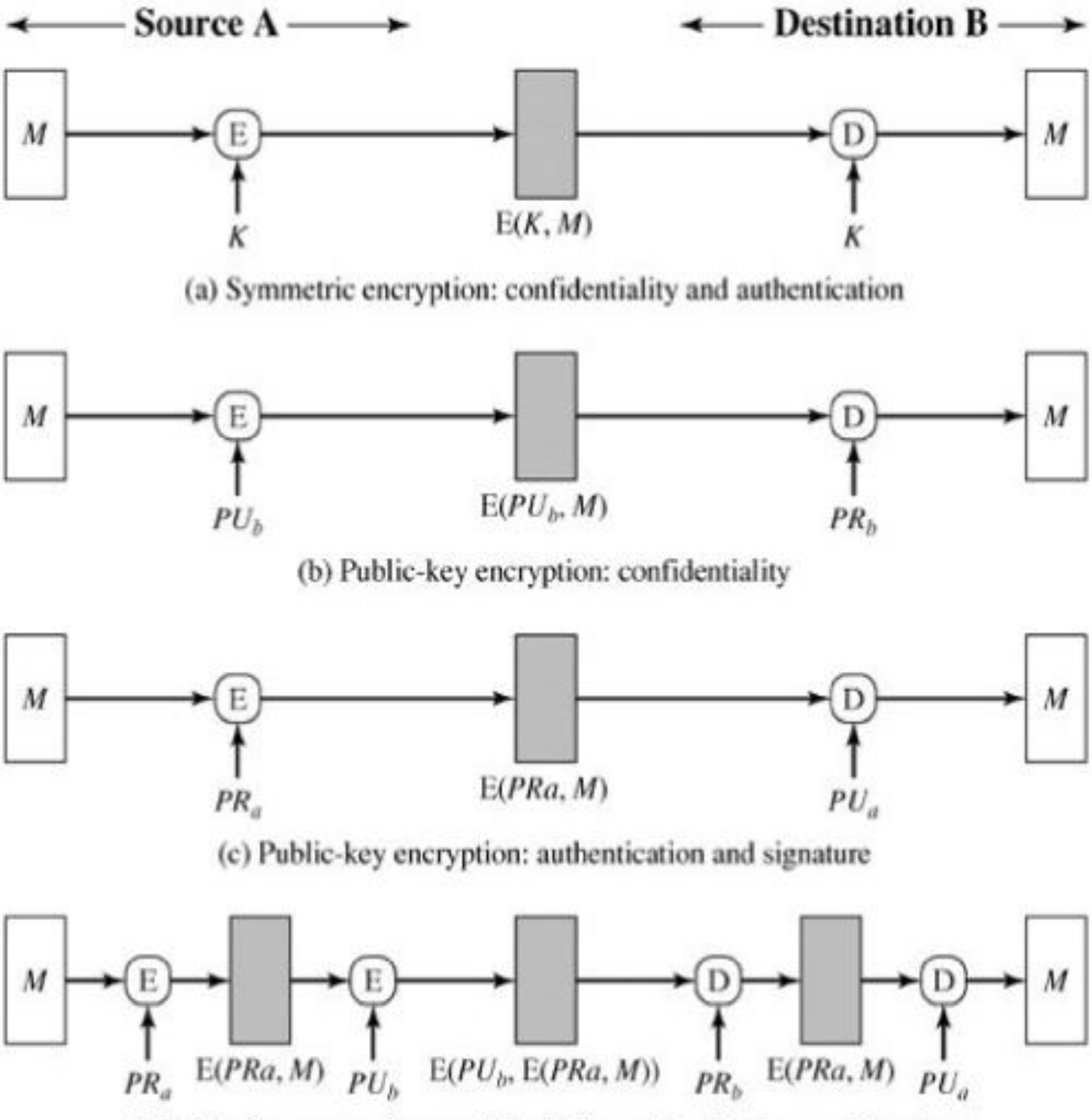
Applications

- Message Authentication
- Digital Signatures
- Other applications
  - one-way password file
  - intrusion detection
  - virus detection
  - pseudorandom number generator
  - etc.

Message Authentication

- Message authentication
  - a mechanism or service used to verify the integrity of a message
    - it assures that data received is exactly as sent
    - the purported identity of the sender is valid.
    - non-repudiation (dispute resolution)
- Message digest – Hash function value
- Techniques used
  - encryption
  - secure hash function.
  - message authentication code (MAC)

Message Encryption



(a) Symmetric encryption: confidentiality and authentication

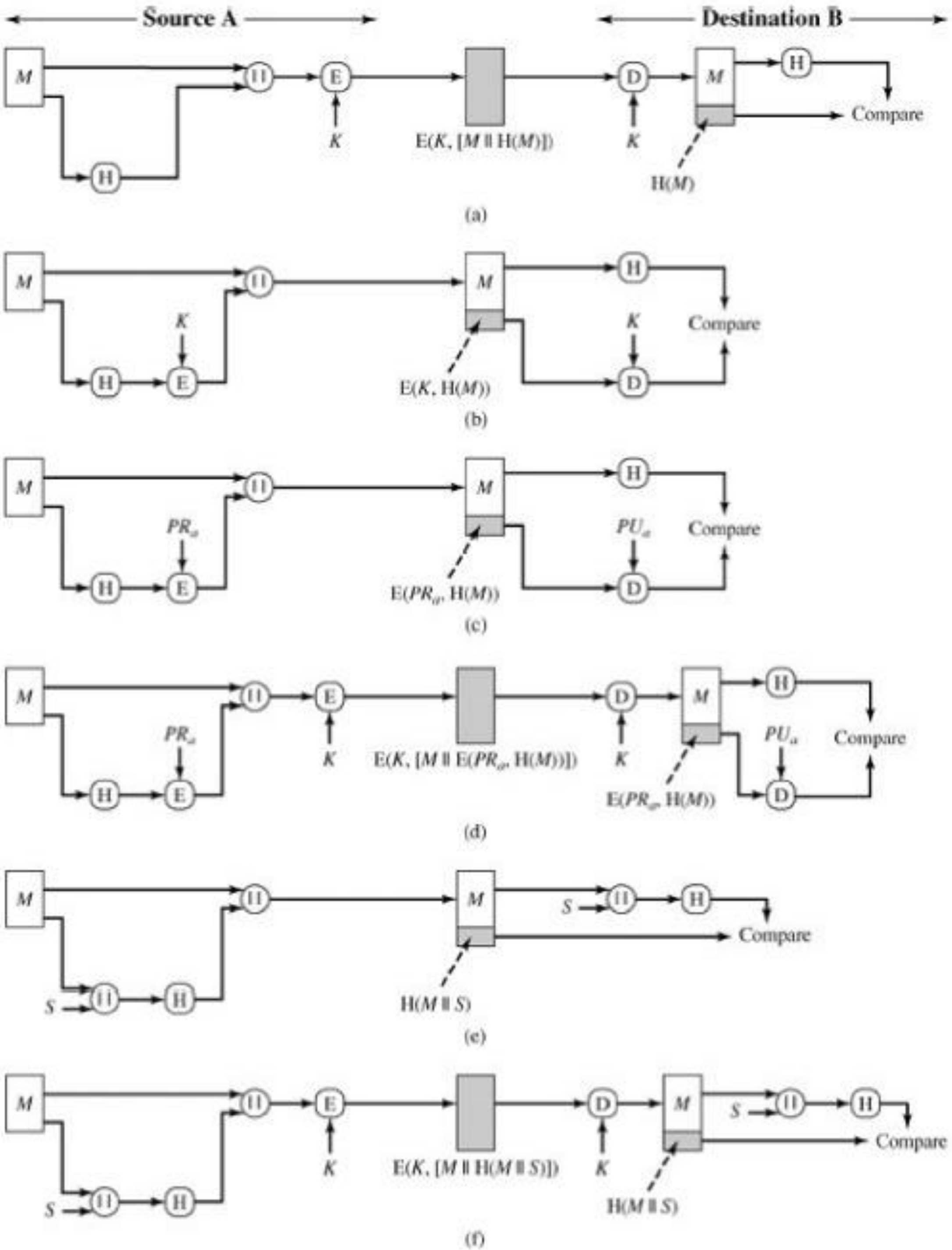
(b) Public-key encryption: confidentiality

(c) Public-key encryption: authentication and signature

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

Why not PU_b then PR_a?

Secure Hash Function



Simple Hash Functions

- XOR
- RXOR
- Technique proposed by National Bureau of Standards

Discussed in the class