CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous class

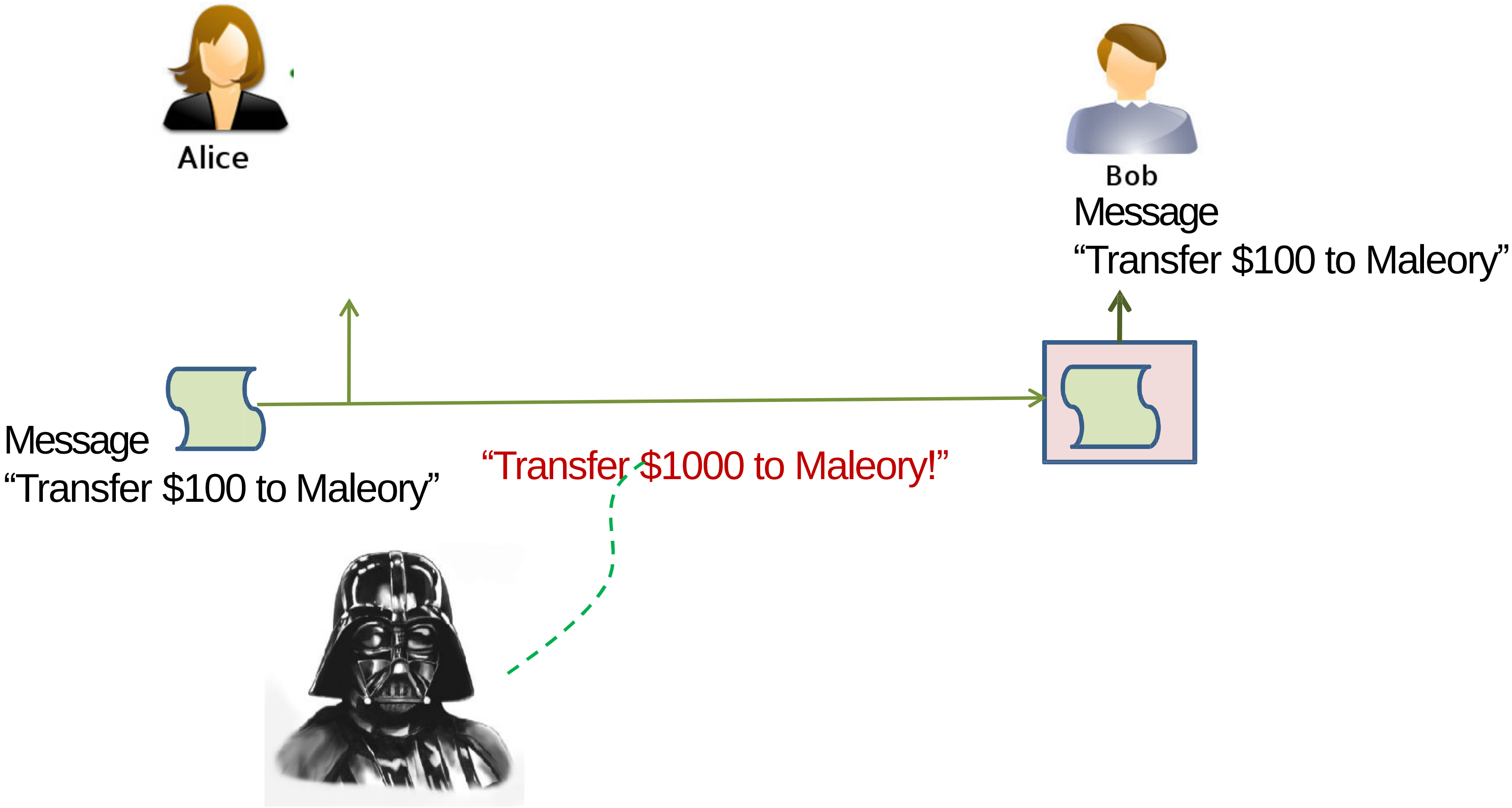
- Crypto Basics
- Cryptographic algorithms
  - important element in security services
- review various types of elements
  - symmetric encryption
  - Hash and MAC

Present class

- Crypto Basics

- review various types of elements
  - Public key encryption

Hash (Manipulation Detection code)



Alice

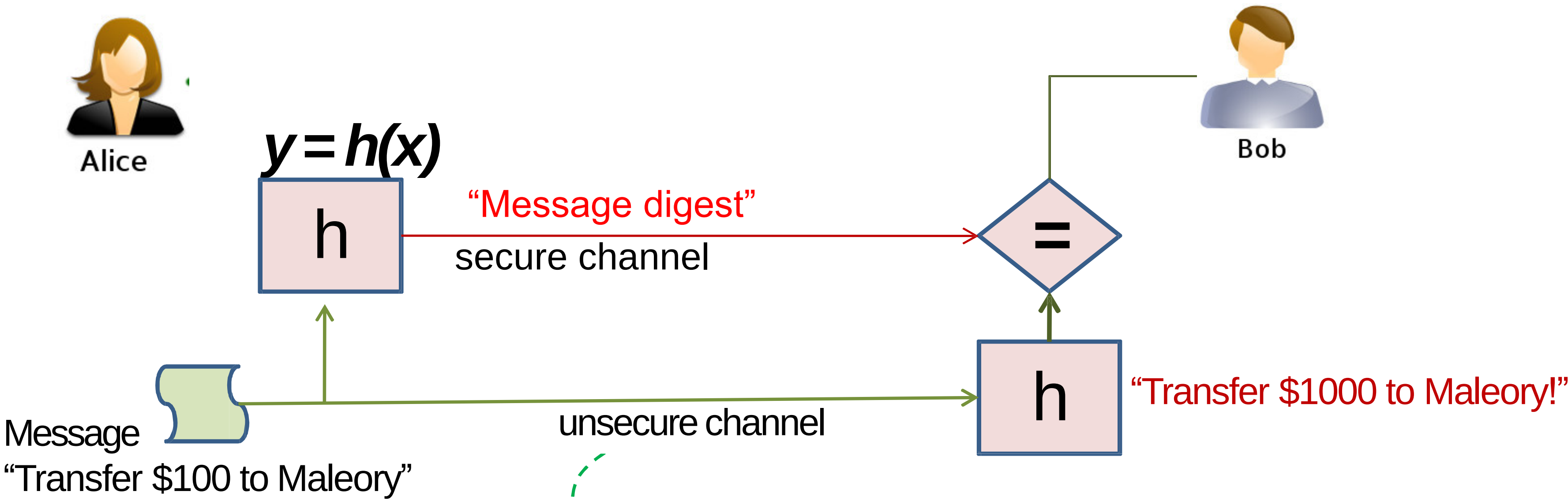
Bob

Message
“Transfer $100 to Maleory”

Message
“Transfer $100 to Maleory”

“Transfer $1000 to Maleory!”

Hash (Manipulation Detection code)



To suceed

Maleory needs to modify x to x′, such that

$$h(x) = h(x')$$

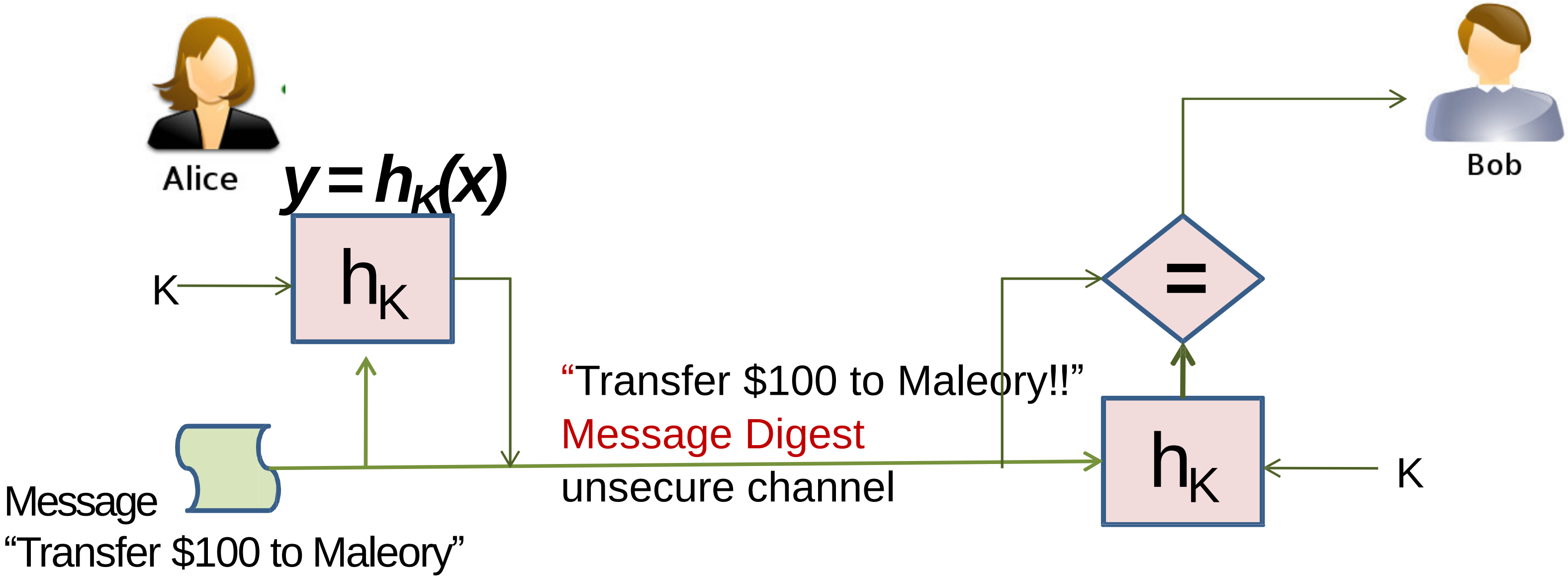
Goal of Hash functions is to resist such collisions

Attacks against MDC

OWHF: given y find x s.t. h(x)=y; or given (x,h(x)) find $x' \neq x$ s.t. $h(x')=h(x)$

CRHF: find any two inputs $x' \neq x$ s.t. $h(x')=h(x)$ (birthday attack)

Message Authentication Codes (MAC)



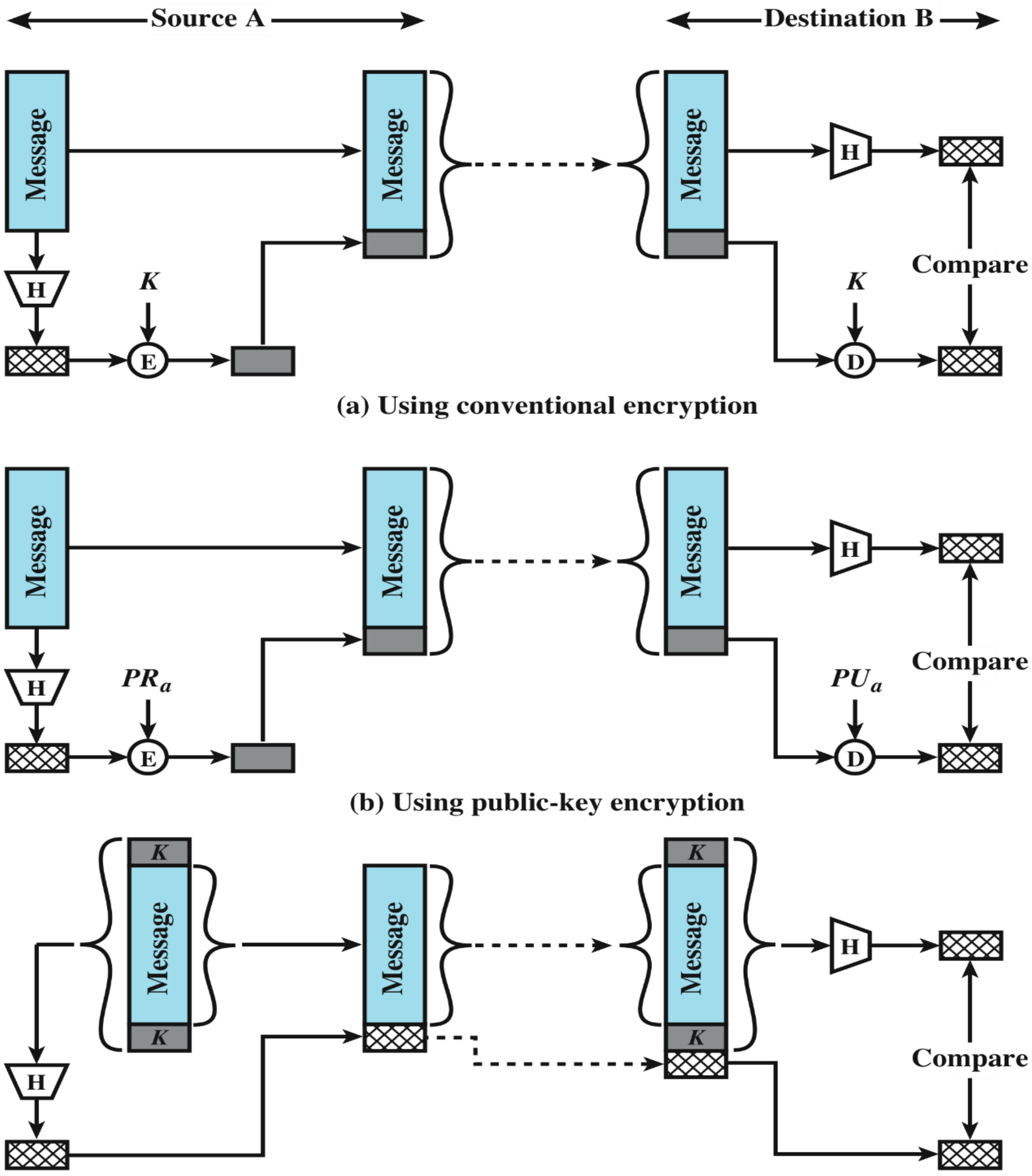
MACs can allow the message and the digest to be sent over an insecure channel

However, it requires Alice and Bob to share a common key

Attacks against MAC

without <u>knowing k</u> compute $(x, h_k(x))$ given $(x_i, h_k(x_i))$ with $x_i \neq x$

Message Authentication Using a One-Way Hash Function

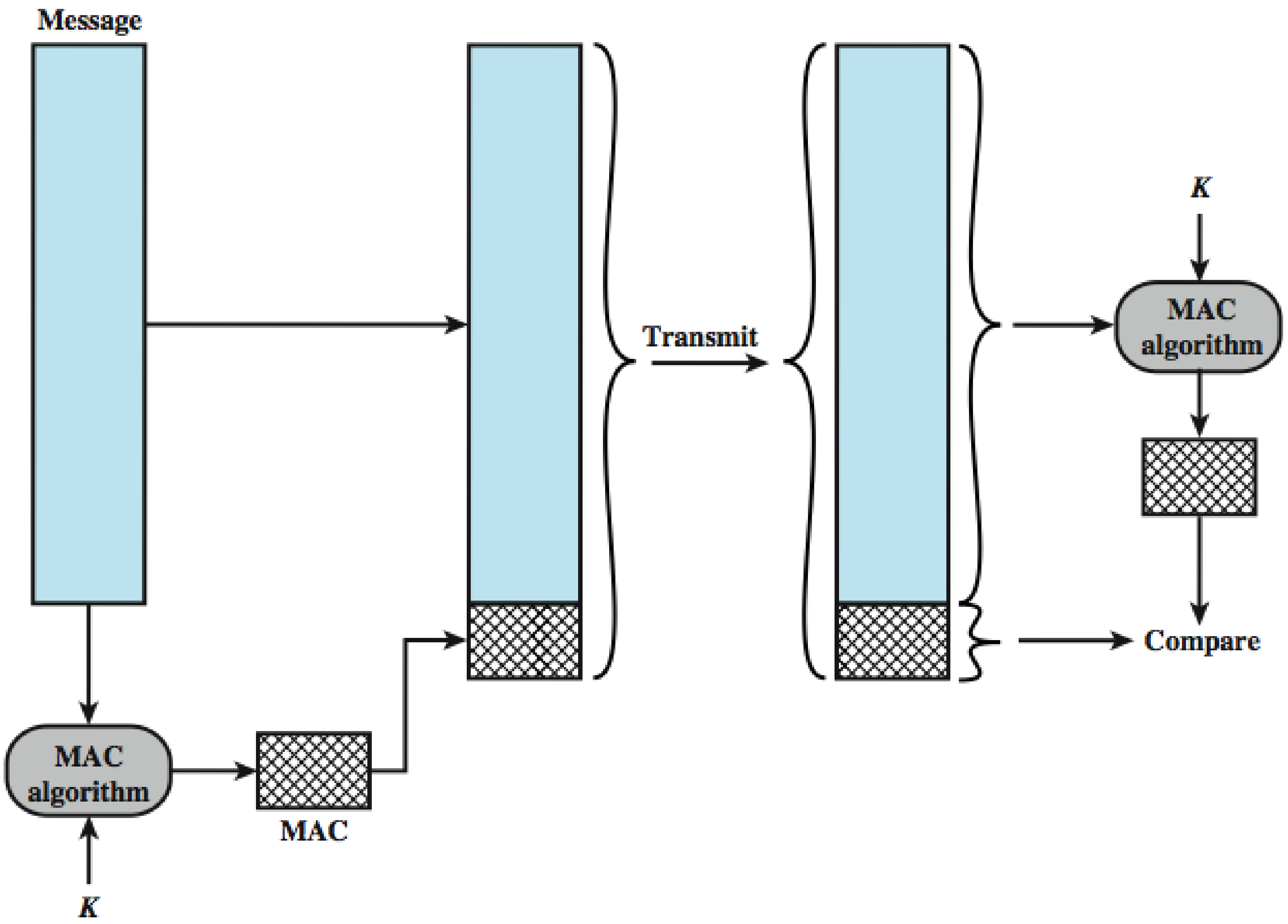


(a) Using conventional encryption

(b) Using public-key encryption

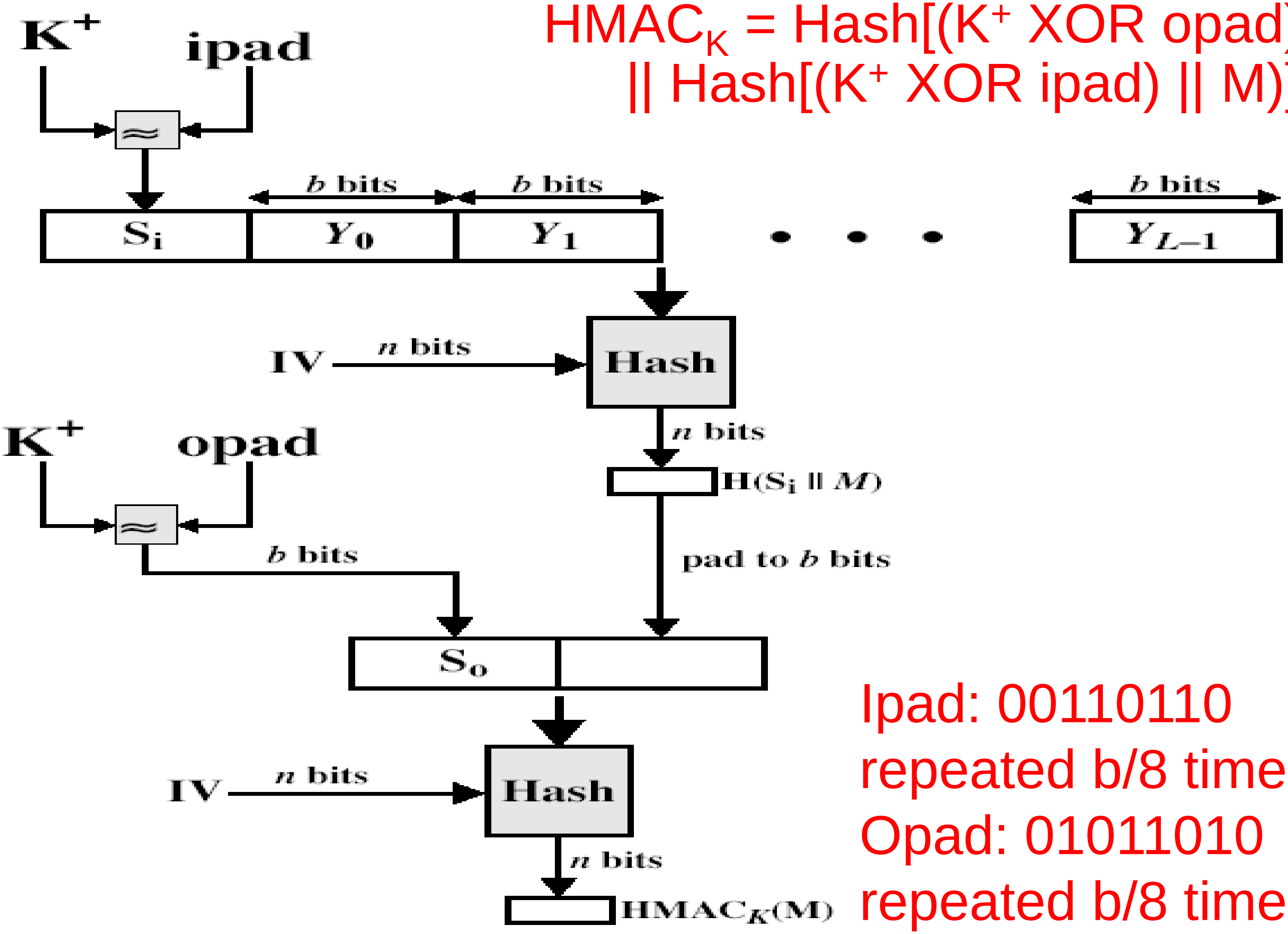
(c) Using secret value

Message Authentication Codes



HMAC Overview

$$HMAC_K = Hash[(K^+ \text{ XOR opad}) \;||\; Hash[(K^+ \text{ XOR ipad}) \;||\; M)]]$$



Ipad: 00110110 repeated b/8 times

Opad: 01011010 repeated b/8 times

Public-Key Encryption Structure

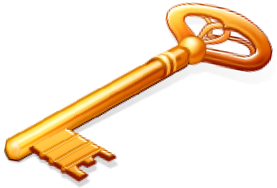
publicly proposed by Diffie and Hellman in 1976

based on mathematical functions

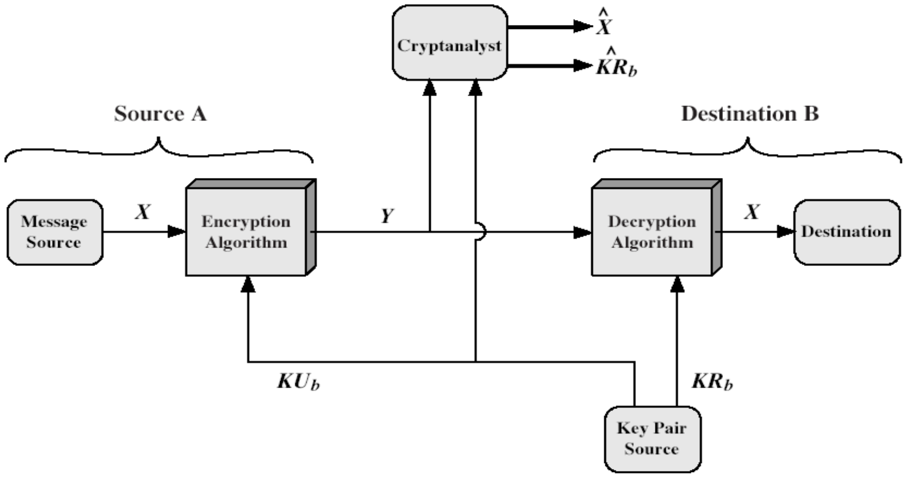
asymmetric

- uses two separate keys
- public key and private key
- public key is made public for others to use

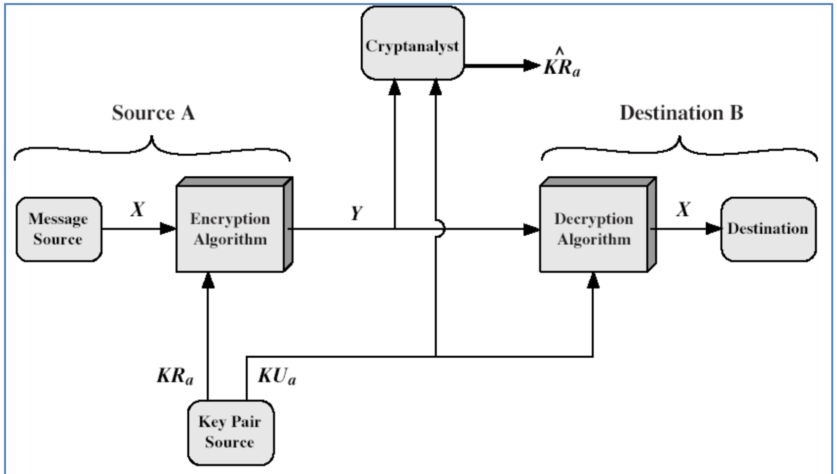
some form of protocol is needed for distribution



Public-Key Cryptosystems



Public-Key Cryptosystem: Secrecy



Public-Key Cryptosystem: Authentication

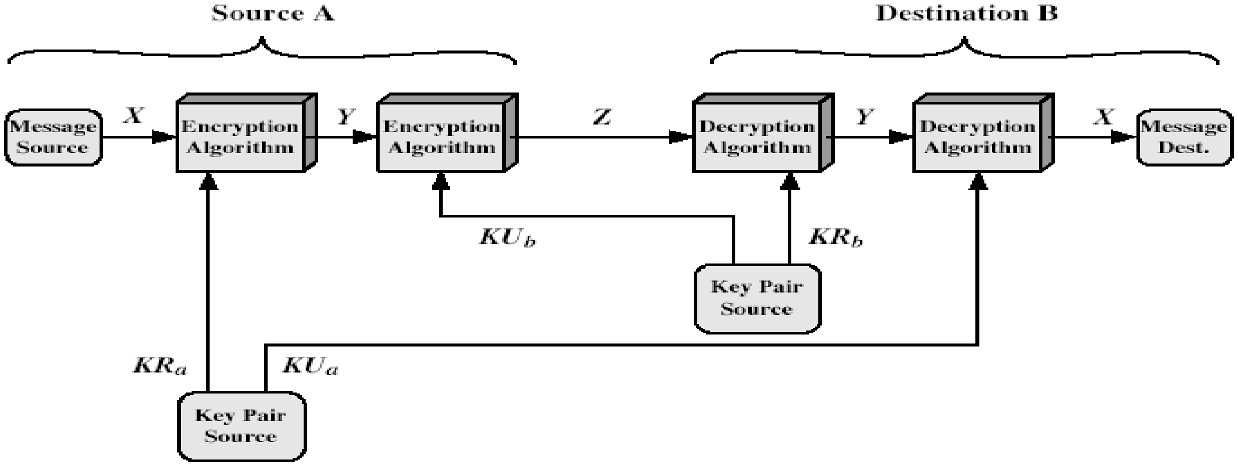


Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

Requirements for Public-Key Crypto.

computationally easy to create key pairs

useful if either key can be used for each role

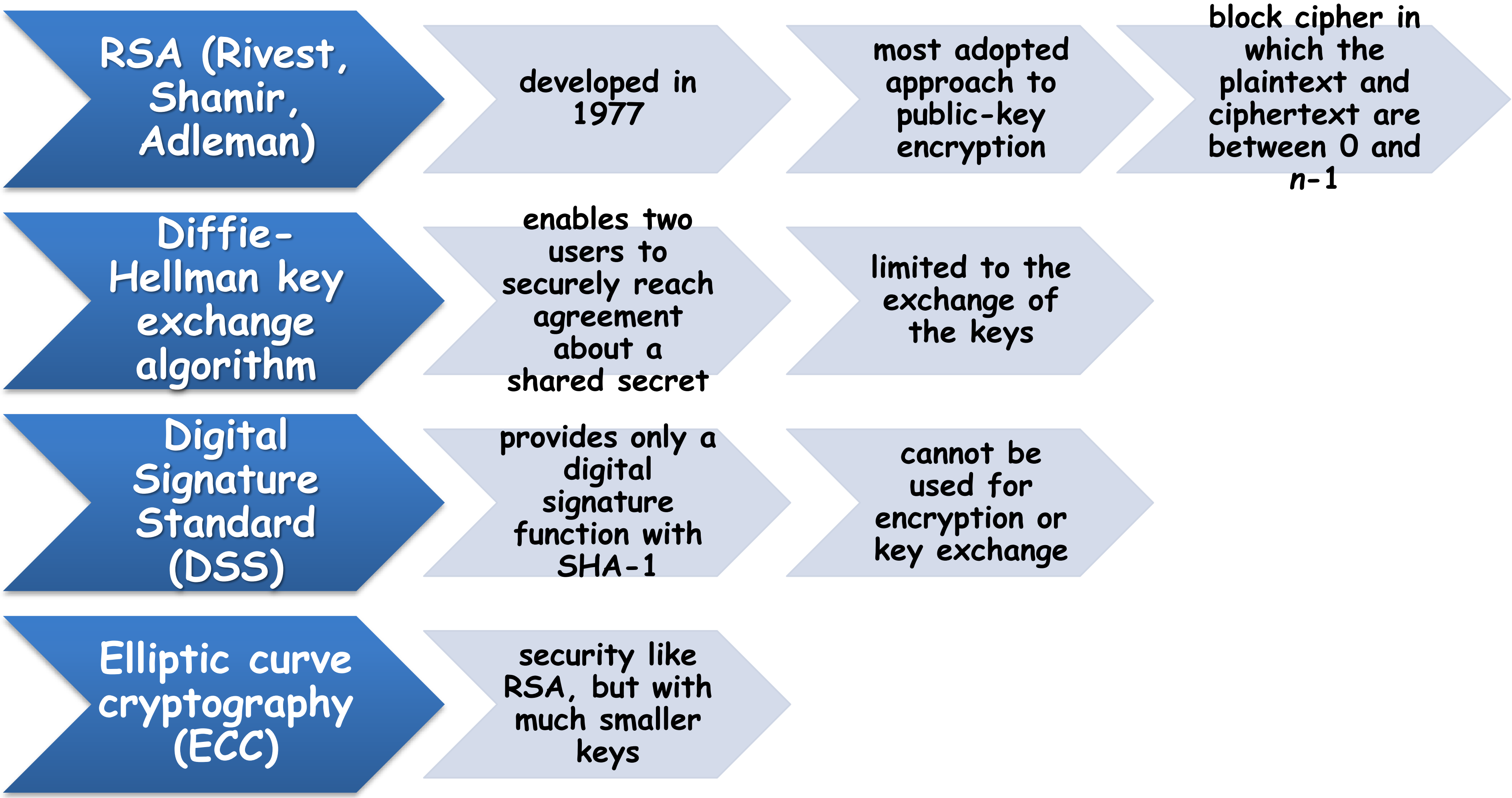
computationally easy for sender knowing public key to encrypt messages

computationally infeasible for opponent to otherwise recover original message

computationally easy for receiver knowing private key to decrypt ciphertext

computationally infeasible for opponent to determine private key from public key

Asymmetric Encryption Algorithms



RSA (Rivest, Shamir, Adleman)

developed in 1977

most adopted approach to public-key encryption

block cipher in which the plaintext and ciphertext are between 0 and *n*−1

Diffie-Hellman key exchange algorithm

enables two users to securely reach agreement about a shared secret

limited to the exchange of the keys

Digital Signature Standard (DSS)

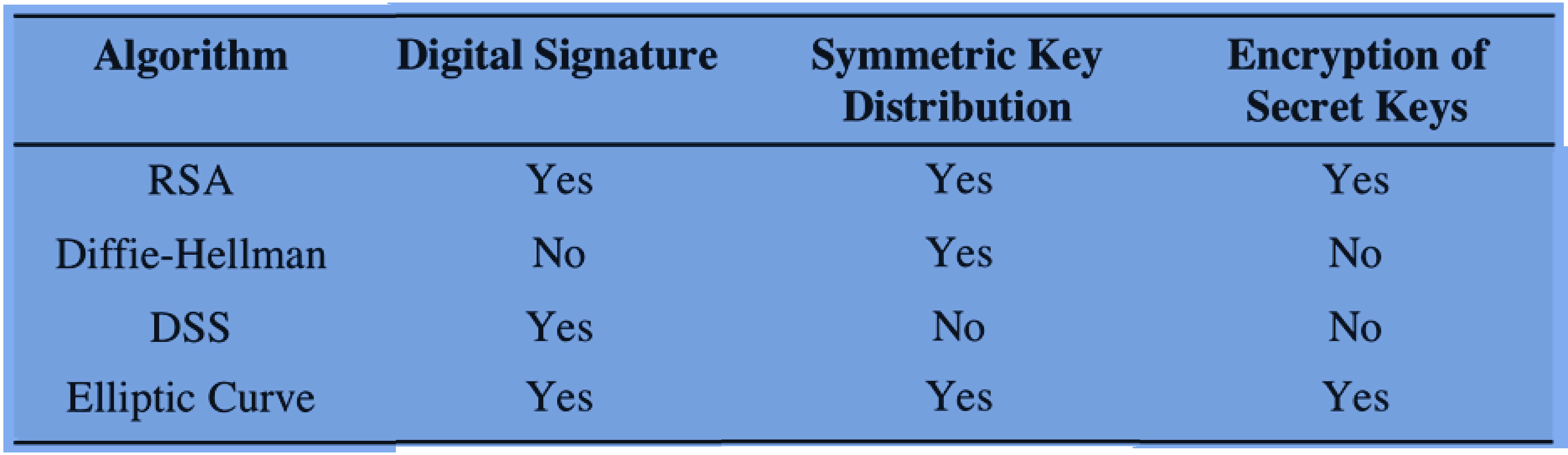
provides only a digital signature function with SHA-1

cannot be used for encryption or key exchange

Elliptic curve cryptography (ECC)

security like RSA, but with much smaller keys

Applications for Public-Key Cryptosystems



Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Thanks