# Chapter 10.1
Cryptography Tools

Book Reading: Computer Security Principles and Practice (3ed), 2015, p.40-66

- cryptographic algorithms important element in security services
- review various types of elements
  - symmetric encryption
  - public-key (asymmetric) encryption
  - digital signatures and key management
  - secure hash functions
- example is use to encrypt stored data
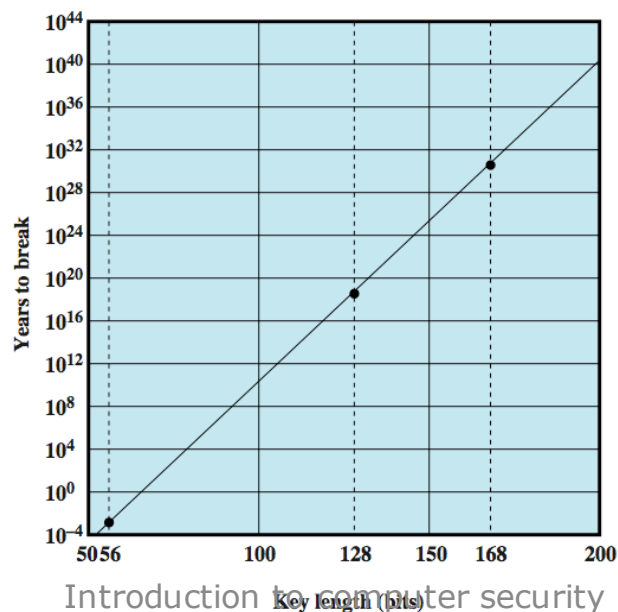
Symmetric Encryption
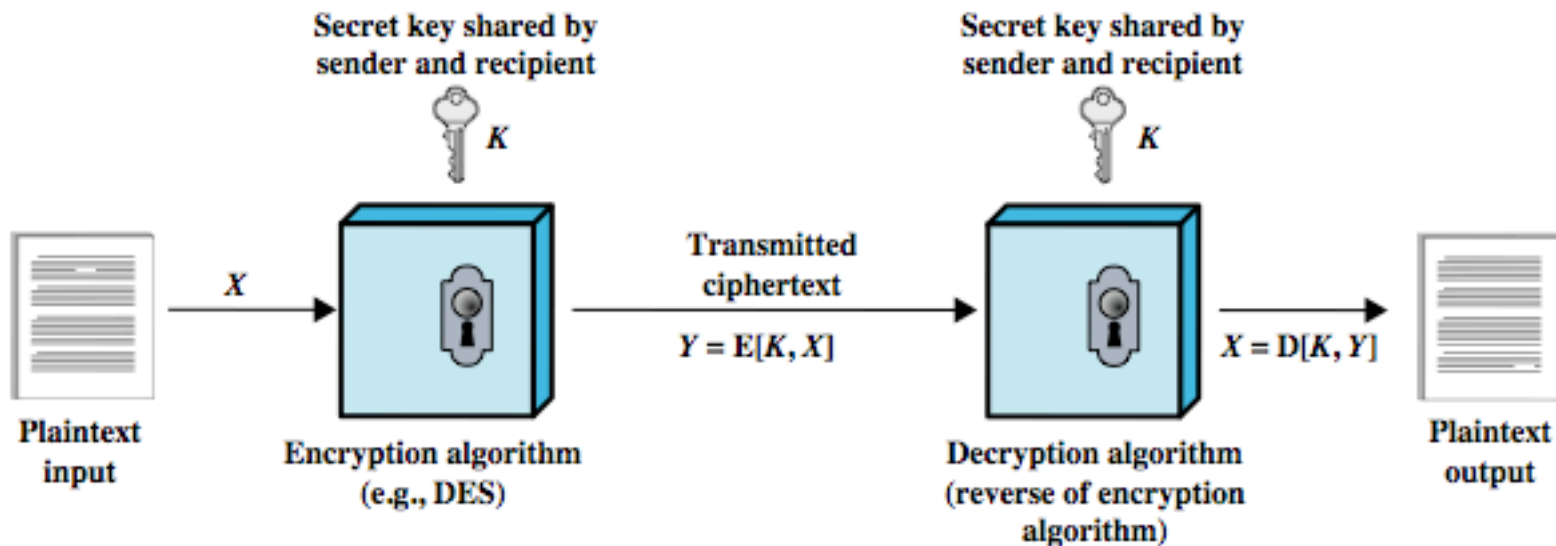
Attacking Symmetric Encryption

- cryptanalysis
  - rely on nature of the algorithm
  - plus some knowledge of plaintext characteristics
  - even some sample plaintext-ciphertext pairs
  - exploits characteristics of algorithm to deduce specific plaintext or key
- brute-force attack
  - try all possible keys on some ciphertext until get an intelligible translation into plaintext

Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs		Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs	= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs	= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs	= 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs	= 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years		6.4×10^6 years

Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

DES and Triple-DES

- Data Encryption Standard (DES) is the most widely used encryption scheme
  - uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
  - concerns about algorithm & use of 56-bit key
- Triple-DES
  - repeats basic DES algorithm three times
  - using either two or three unique keys
  - much more secure but also much slower

# Advanced Encryption Standard (AES)

- needed a better replacement for DES
- NIST called for proposals in 1997
  - efficiency, security, HW/SW suitability, 128, 256, 256 keys
- selected Rijndael in Nov 2001
- symmetric block cipher
- uses 128 bit data & 128/192/256 bit keys
- now widely available commercially

Block verses Stream Ciphers
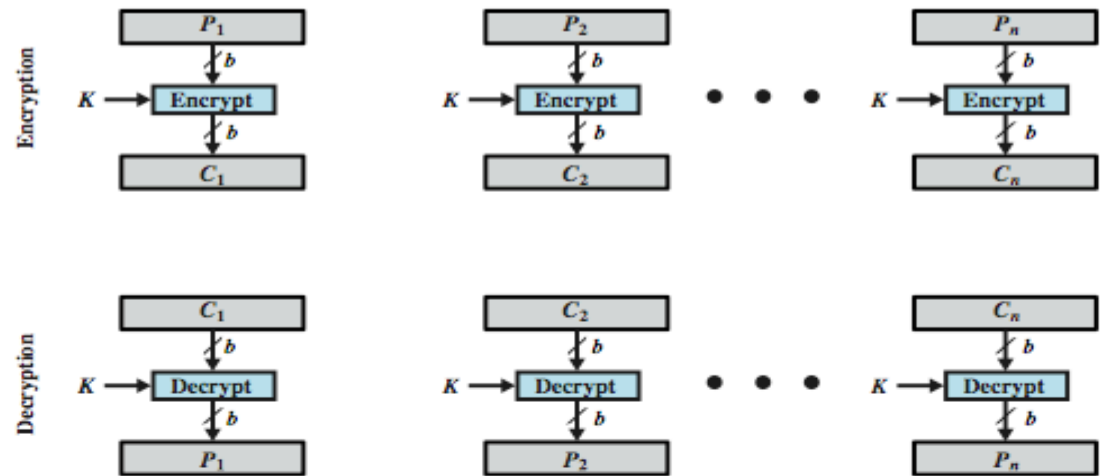
(a) Block cipher encryption (electronic codebook mode)
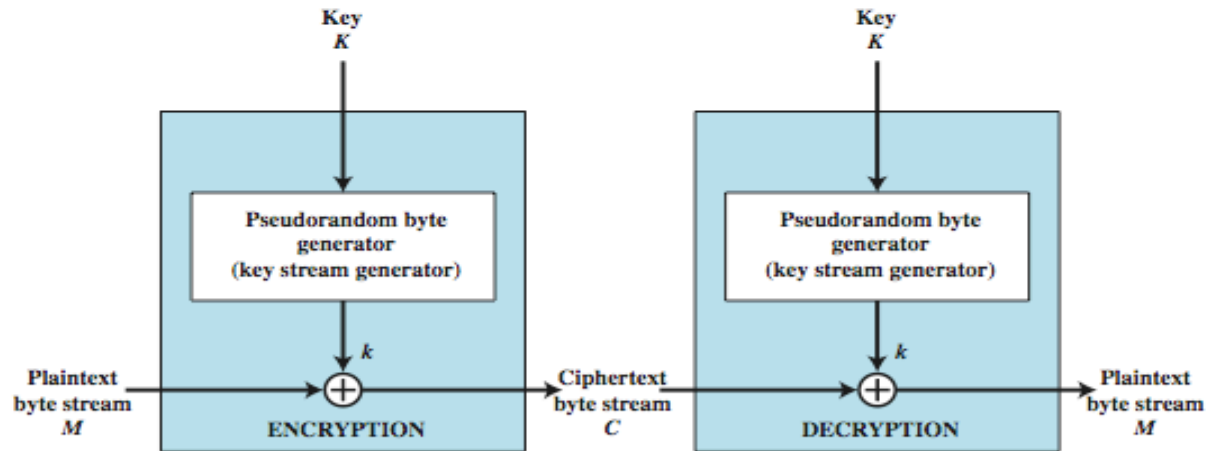

(b) Stream encryption

Message Authentication

- protects against active attacks
- verifies received message is authentic
  - contents unaltered
  - from authentic source
  - timely and in correct sequence
- can use conventional encryption
  - only sender & receiver have key needed
- or separate authentication mechanisms
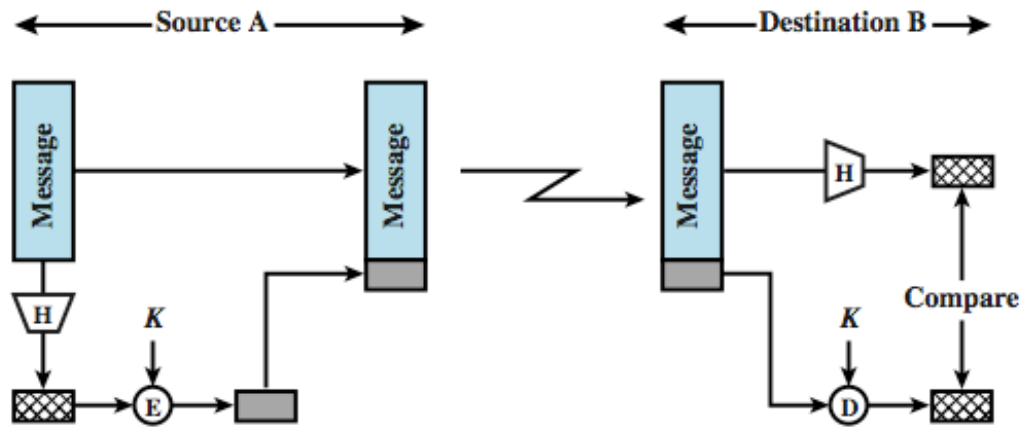 - append authentication tag to cleartext message
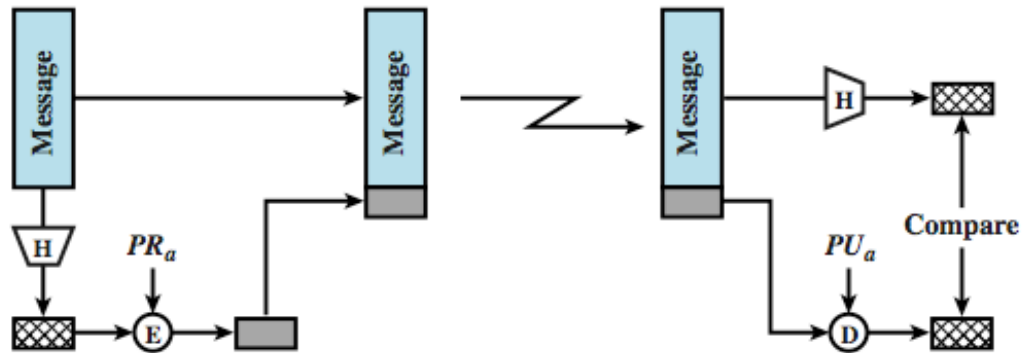
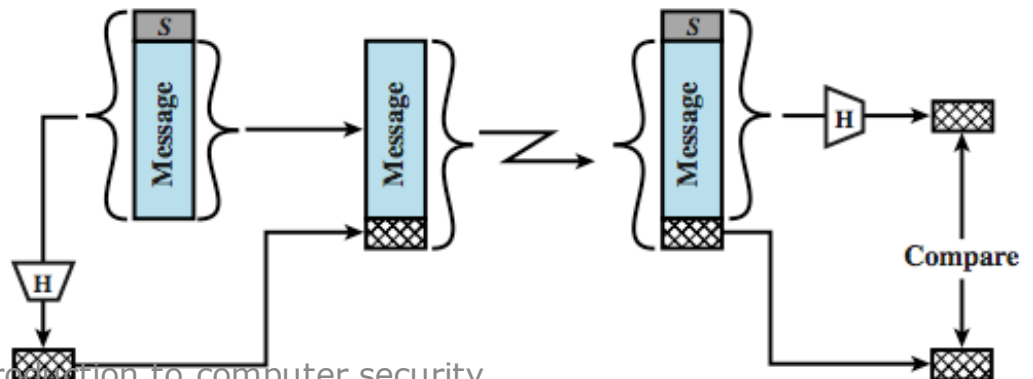# Message Authentication Codes
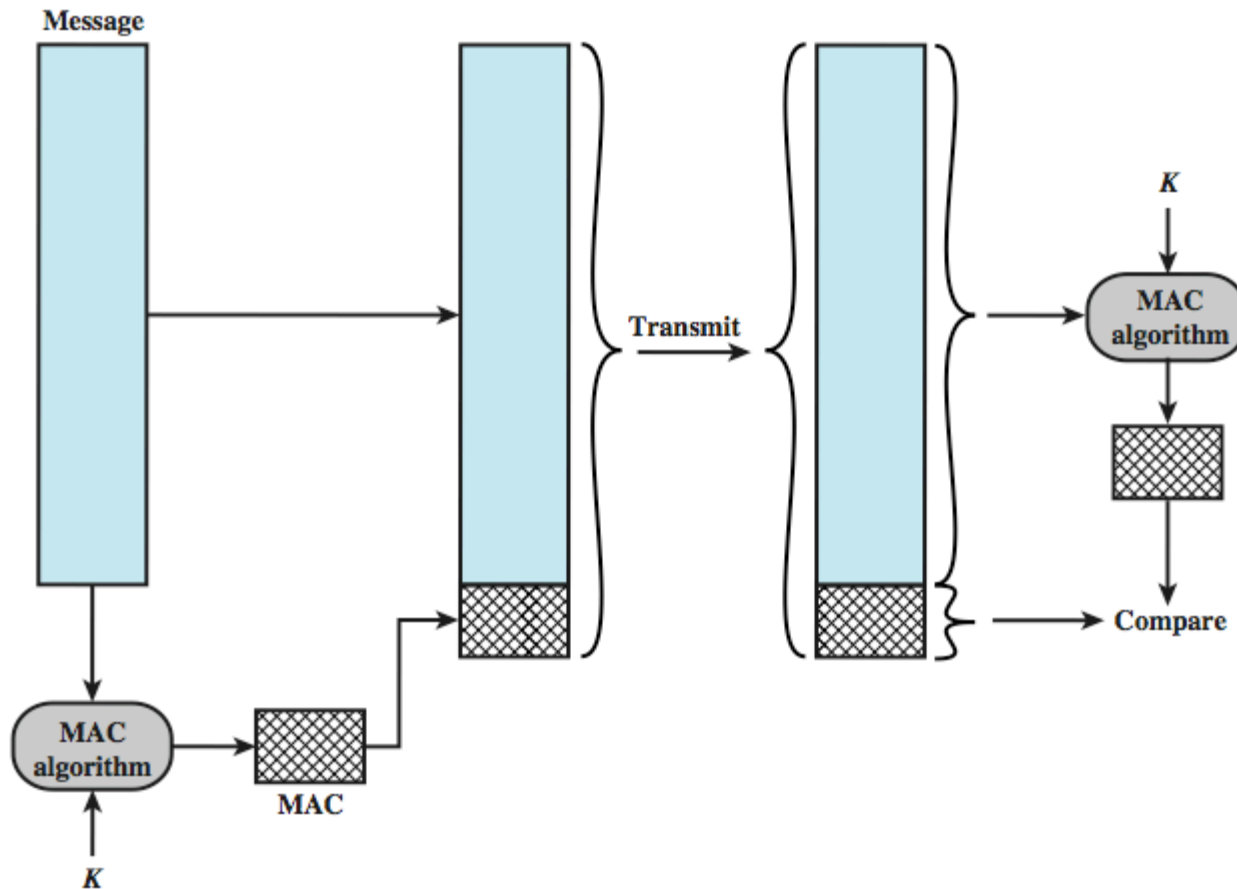
Secure Hash Functions

Message or data block *M*
(variable length)

H

Hash value *h*
fixed length)
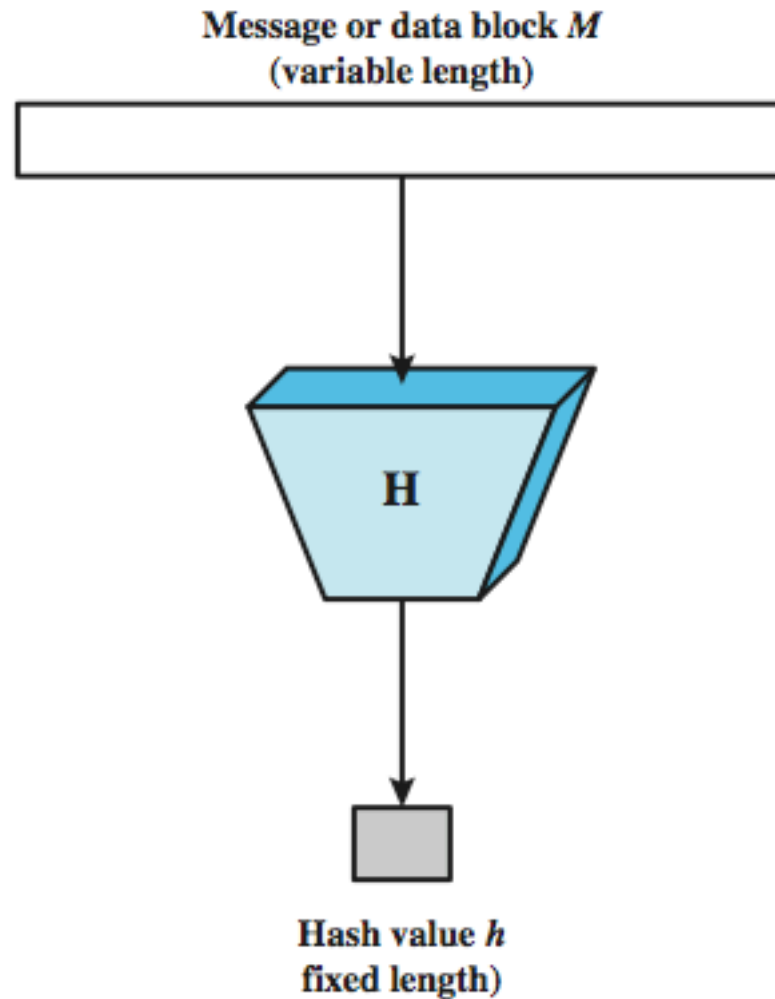
Message Auth

(a) Using conventional encryption
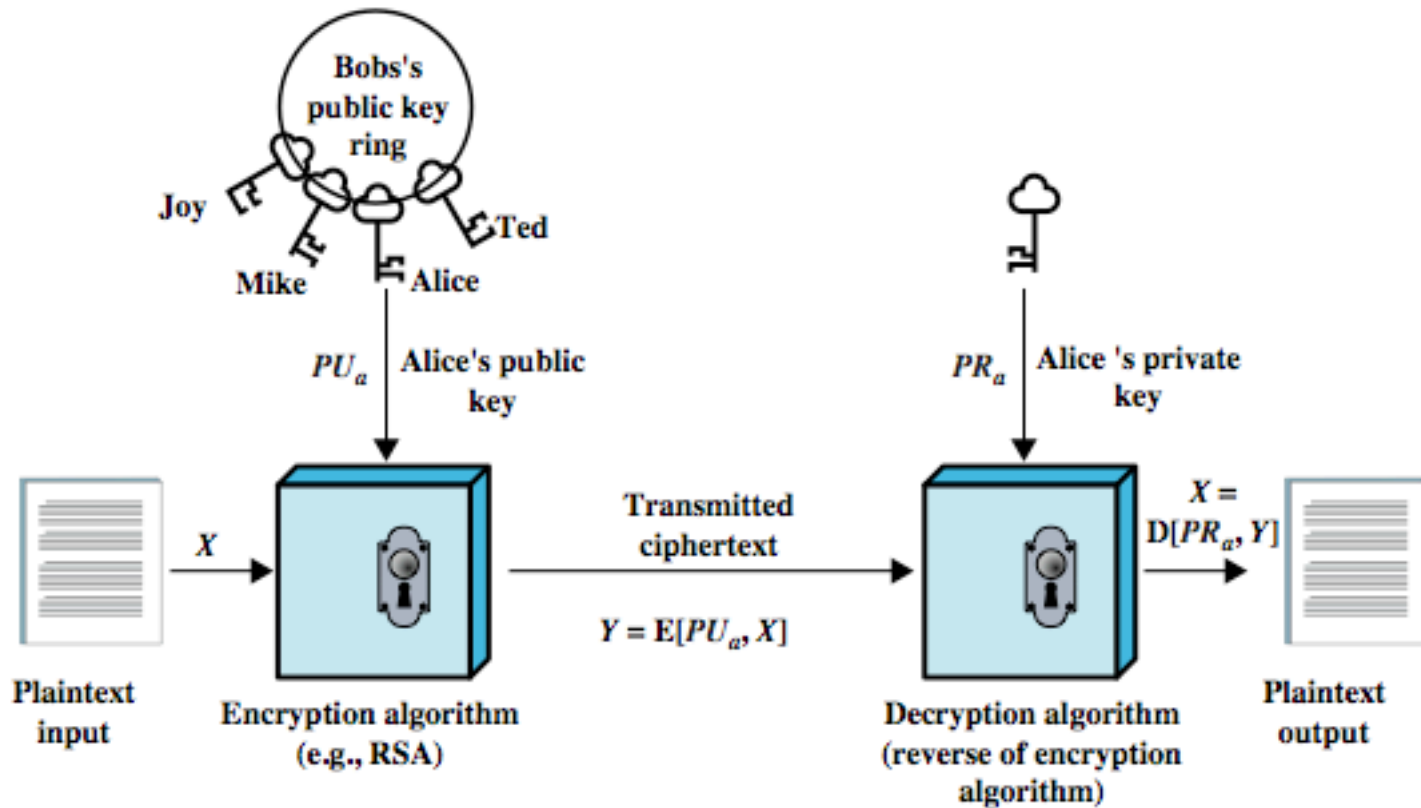
(b) Using public-key encryption

(c) Using secret value

Hash Function Requirements

- applied to any size data
- H produces a fixed-length output.
- $H(x)$ is relatively easy to compute for any given x
- one-way property
  - computationally infeasible to find x such that $H(x) = h$
- weak collision resistance
  - computationally infeasible to find $y \neq x$ such tha $H(y) = H(x)$
- strong collision resistance
  - computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$

Hash Functions

- two attack approaches
  - cryptanalysis
    - exploit logical weakness in alg
  - brute-force attack
    - trial many inputs
    - strength proportional to size of hash code ($2^{n/2}$)
- SHA most widely used hash algorithm
  - SHA-1 gives 160-bit hash
  - more recent SHA-256, SHA-384, SHA-512 provide improved size and security
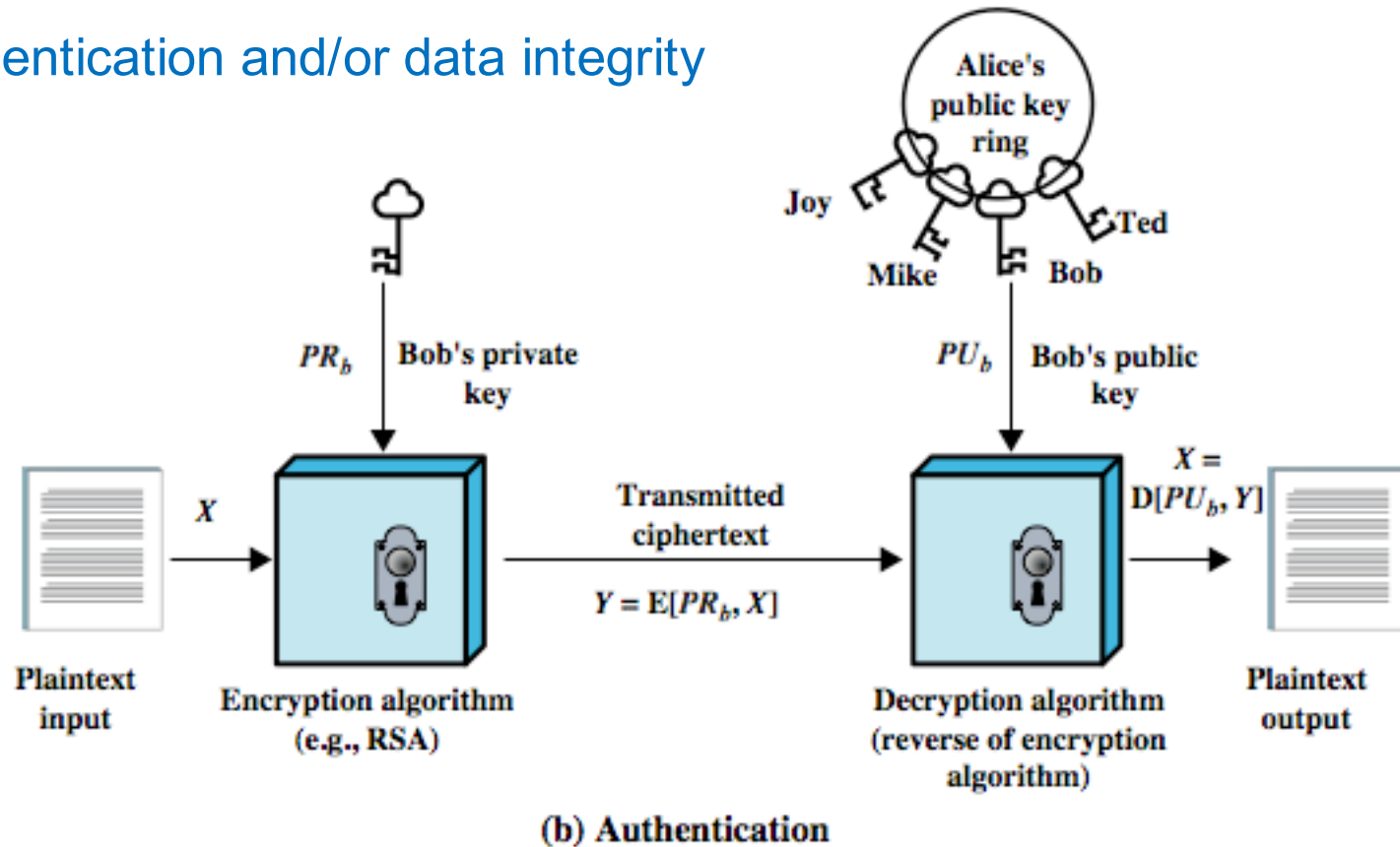
Public Key Encryption

(a) Confidentiality

Public Key Authentication

Authentication and/or data integrity

(b) Authentication

Public Key Requirements

1. computationally easy to create key pairs
2. computationally easy for sender knowing public key to encrypt messages
3. computationally easy for receiver knowing private key to decrypt ciphertext
4. computationally infeasible for opponent to determine private key from public key
5. computationally infeasible for opponent to otherwise recover original message
6. useful if either key can be used for each role

Public Key Algorithms

- RSA (Rivest, Shamir, Adleman)
  - developed in 1977
  - only widely accepted public-key encryption alg
  - given tech advances need 1024+ bit keys
- Diffie-Hellman key exchange algorithm
  - only allows exchange of a secret key
- Digital Signature Standard (DSS)
  - provides only a digital signature function with SHA-1
- Elliptic curve cryptography (ECC)
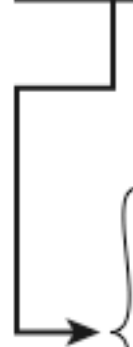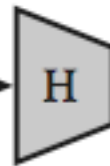 - new, security like RSA, but with much smaller keys

Public Key Certificates

Unsigned certificate:
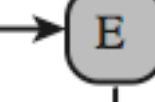contains user ID,
user's public key

Generate hash
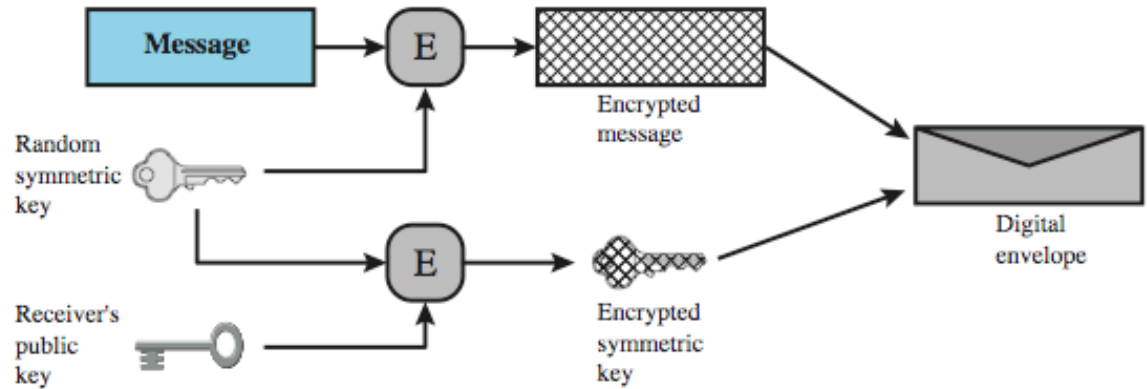code of unsigned
certificate

See textbook figure p.63

H

Encrypt hash code
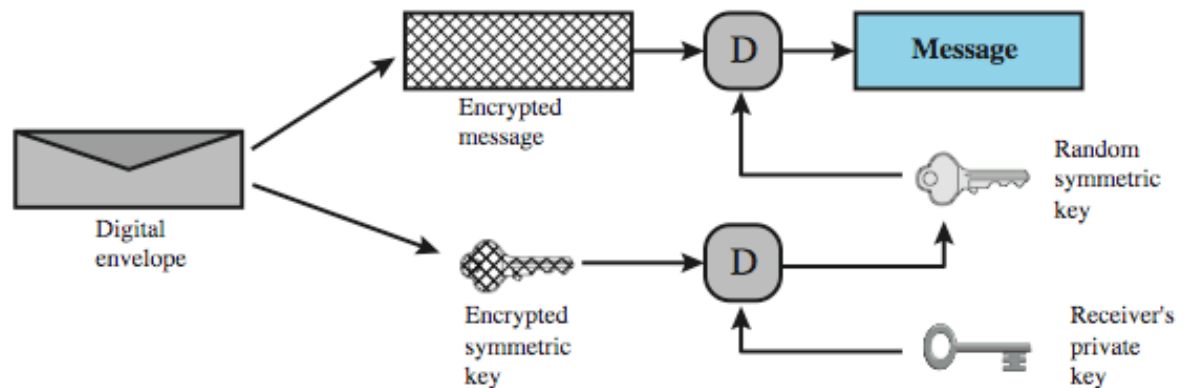with CA's private key
to form signature

E

Signed certificate:
Recipient can verify
signature using CA's
public key.

Digital Envelopes

(a) Creation of a digital envelope

(b) Opening a digital envelope

Another application of public key alg

Random Numbers

- random numbers have a range of uses

- requirements:

- randomness
  - based on statistical tests for uniform distribution and independence

- unpredictability
  - successive values not related to previous
  - clearly true for truly random numbers
  - but more commonly use generator

Pseudorandom verses Random Numbers

- often use algorithmic technique to create pseudorandom numbers
  - which satisfy statistical randomness tests
  - but likely to be predictable
- true random number generators use a nondeterministic source
  - e.g. radiation, gas discharge, leaky capacitors
  - increasingly provided on modern processors

Practical Application: Encryption of Stored Data

- common to encrypt transmitted data
- much less common for stored data
  - which can be copied, backed up, recovered
- approaches to encrypt stored data:
  - back-end appliance *(hardware device close to data storage; encrypt close to wire speed)*
  - library based tape encryption *(co-processor board embedded in tape drive)*
  - background laptop/PC data encryption

Summary

- introduced cryptographic algorithms
- symmetric encryption algorithms for confidentiality
- message authentication & hash functions
- public-key encryption
- digital signatures and key management
- random numbers