CNET233SL – Network Security

Cryptographic Tools

saliya@nsbm.lk

Outline

- Cryptanalysis
- Symmetric encryption
- Substitution Ciphers (Shift, Transposition)
- Message integrity check (MAC, Hash)
- Public key cryptography
- Digital Signatures
- The RSA Public-Key Encryption Algorithm

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)-** recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology -** field of both cryptography and cryptanalysis

Cryptography

- can characterise cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - product
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack
- if either succeed all key use compromised

Cryptanalytic attack Vs Brute-force attack

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful all future and past messages encrypted with that key are compromised

Brute-Force Attack

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - On average half of all possible keys must be tried to achieve success

Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text**
  - select plaintext or ciphertext to en/decrypt

- An encryption scheme: computationally secure if
  - The cost of breaking the cipher exceeds the value of information
  - The time required to break the cipher exceeds the lifetime of information

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

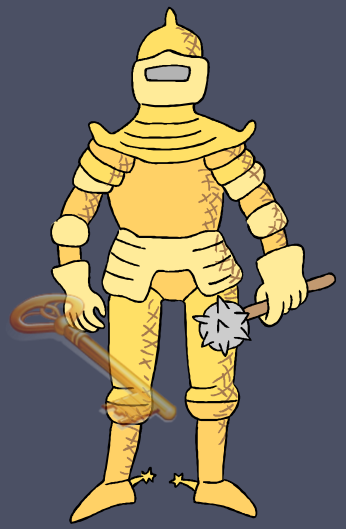
Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4.3 \times 109$	231 µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 1016$	255 µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 1038$	2127 µs = 5.4×1024 years	5.4×1018 years
168	$2^{168} = 3.7 \times 1050$	2167 µs = 5.9×1036 years	5.9×1030 years
26 characters (permutation)	$26! = 4 \times 1026$	2×1026 µs = 6.4×1012 years	6.4×106 years

Encryption

- There are two major categories of encryption schemes
  - **Symmetric Encryption**
    - Also called conventional / private-key / single-key
  - **Asymmetric Encryption**
    - Also called public-key cryptography

Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements for secure use:
  - Need a strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure



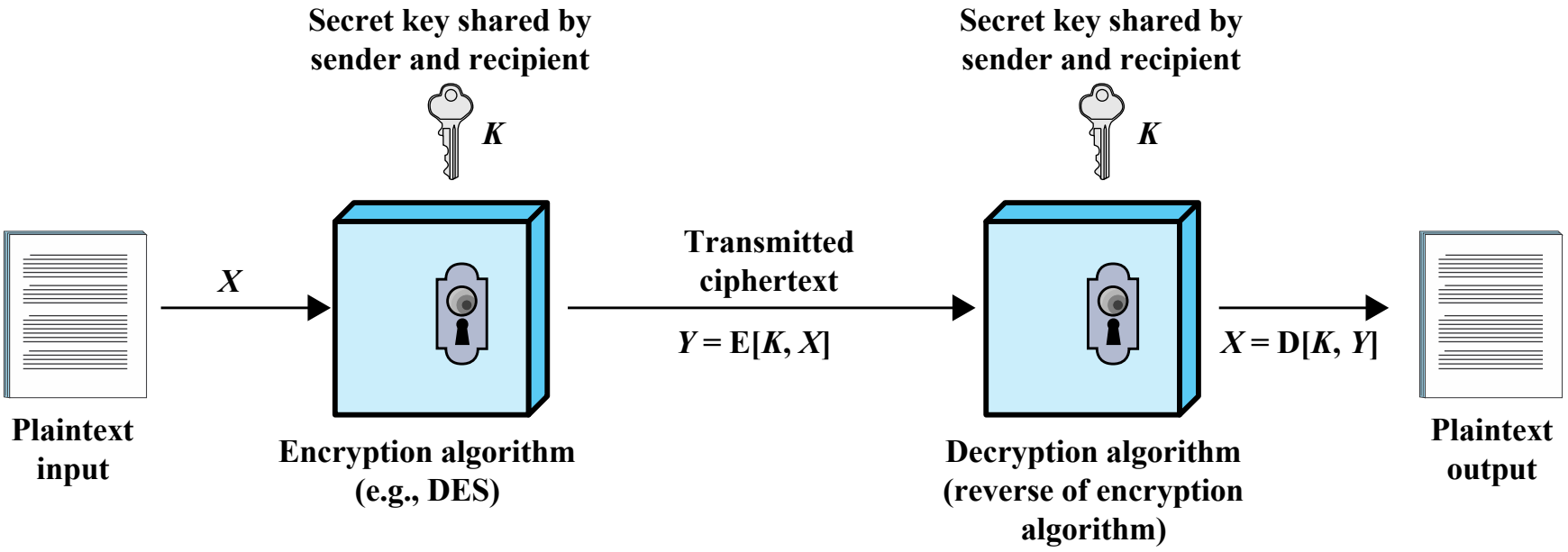


Figure 2.1 Simplified Model of Symmetric Encryption

Shift Ciphers

- Is a very simple substitution *cipher*.
- 'shift' the letter A some number of spaces to the right or left depending on value and the sign of the key, and start the alphabet from there, wrapping around when we get to Z.
- The way in which the shifted alphabet lines up with the un-shifted alphabet is the cipher. For example, a three shift to the left looks like

plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- **Here +3 is the key**

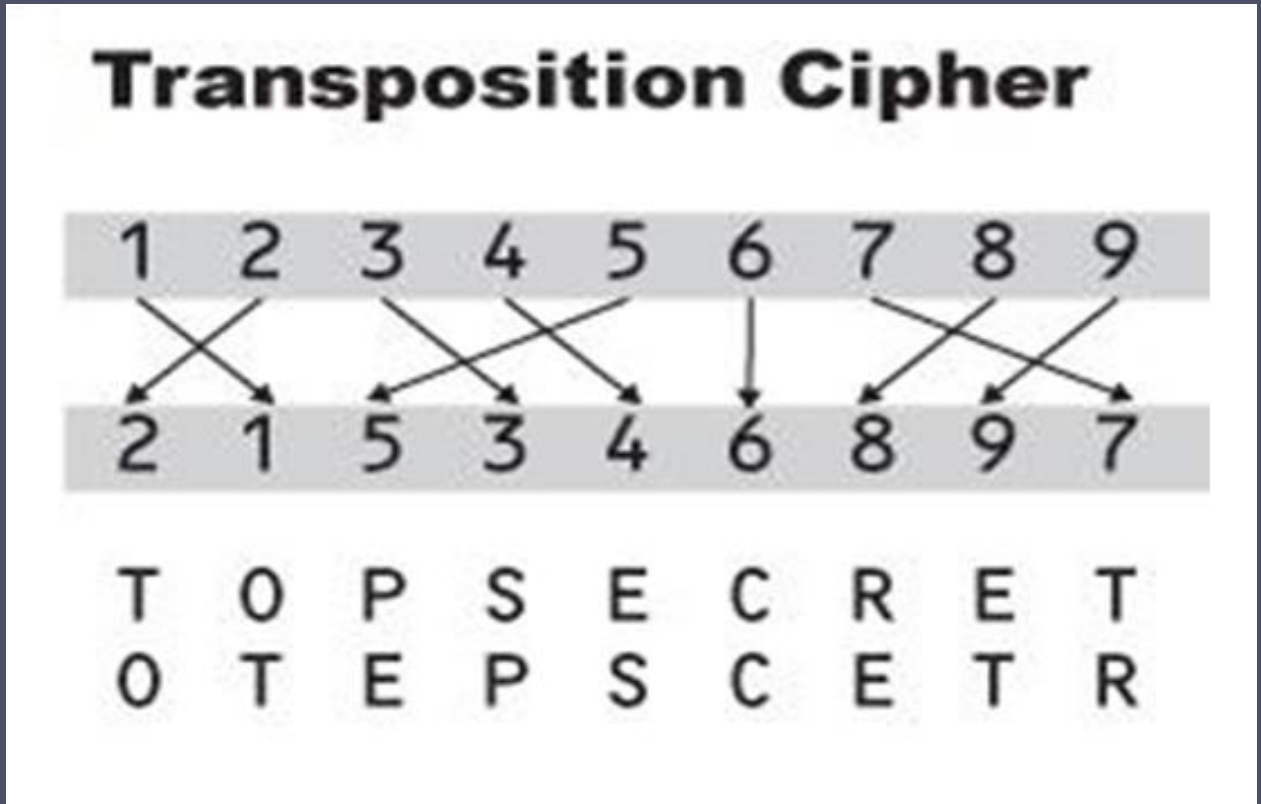
Example

- The message:
  - what kind of cake should we have? alice.
- Encrypted message:
  - ZKDW NLQG RI FDNH VKRXOG ZH KDYH? DOLFH
- How do we go about decrypting this message? It's easy, we just swap the roles of the alphabets above:

ciphertext:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Transposition Ciphers

- Transposition ciphers operate by moving plaintext characters to new locations in the ciphertext, rather than by substituting individual characters.
- Example



- Plain Text
- Cipher Text

- With the availability of computers shift cipher and transposition cipher explain above can be broken effortlessly.

Comparison of Three Currently Popular Symmetric Encryption Algorithms

Table 2.1

	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

Data Encryption Standard (DES)

- The most widely used encryption scheme
  - FIPS PUB 46
  - Referred to as the Data Encryption Algorithm (DEA)
  - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block

- Strength concerns:
  - Concerns about algorithm
    - DES is the most studied encryption algorithm in existence
  - Use of 56-bit key
    - Electronic Frontier Foundation (EFF) announced in July 1998 that it had broken a DES encryption

Table 2.2

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years

Average Time Required for Exhaustive Key Search (i.e. Brute Force Attack)

Triple DES (3DES)

- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
  - 168-bit key length overcomes the vulnerability to brute-force attack of DES
  - Underlying encryption algorithm is the same as in DES
- Drawbacks:
  - Algorithm is sluggish in software
  - Uses a 64-bit block size

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

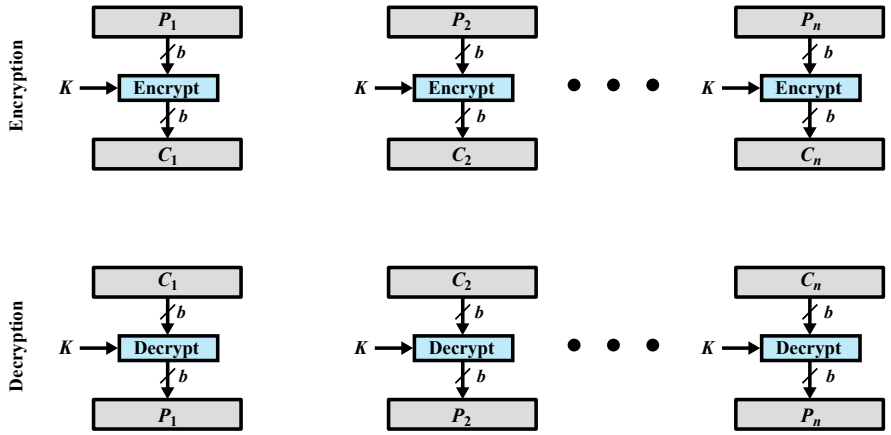
- Should have a security strength equal to or better than 3DES
- Significantly improved efficiency
- Symmetric block cipher
- 128 bit data and 128/192/256 bit keys

Selected Rijndael in November 2001

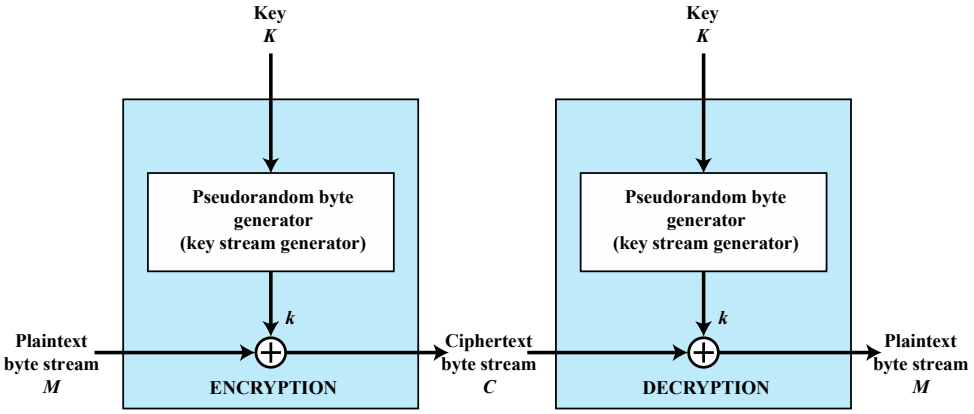
Published as FIPS 197

Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
  - Alternative techniques developed to increase the security of symmetric block encryption for large sequences
  - Overcomes the weaknesses of ECB



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 Types of Symmetric Encryption

Block & Stream Ciphers

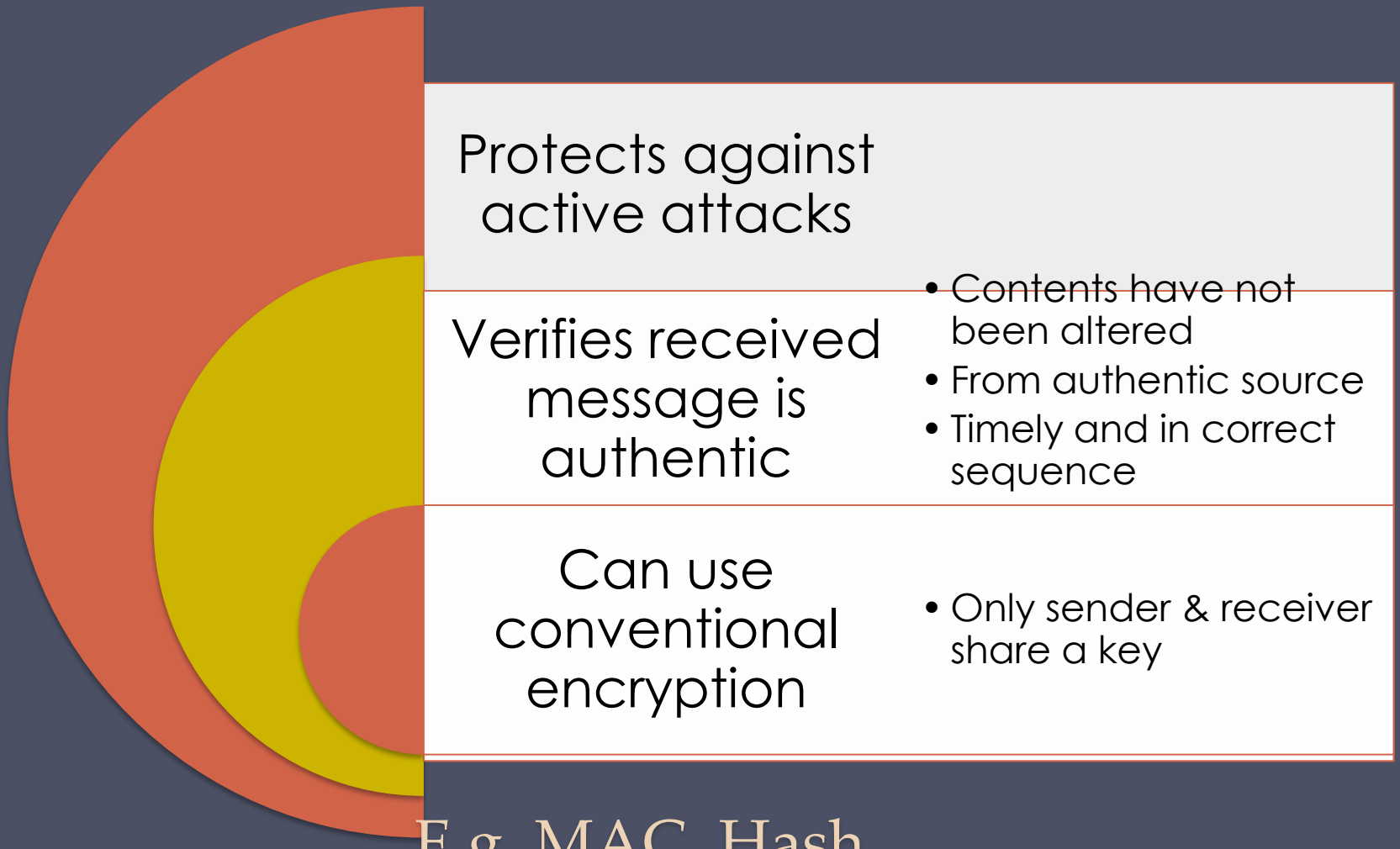
Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

Message Authentication



MAC

- condenses arbitrary message to fixed size
- A secret key is used
- MAC = H(M,K)
- usually assume hash function is public
- MAC used to detect changes to message
- E.g HMAC

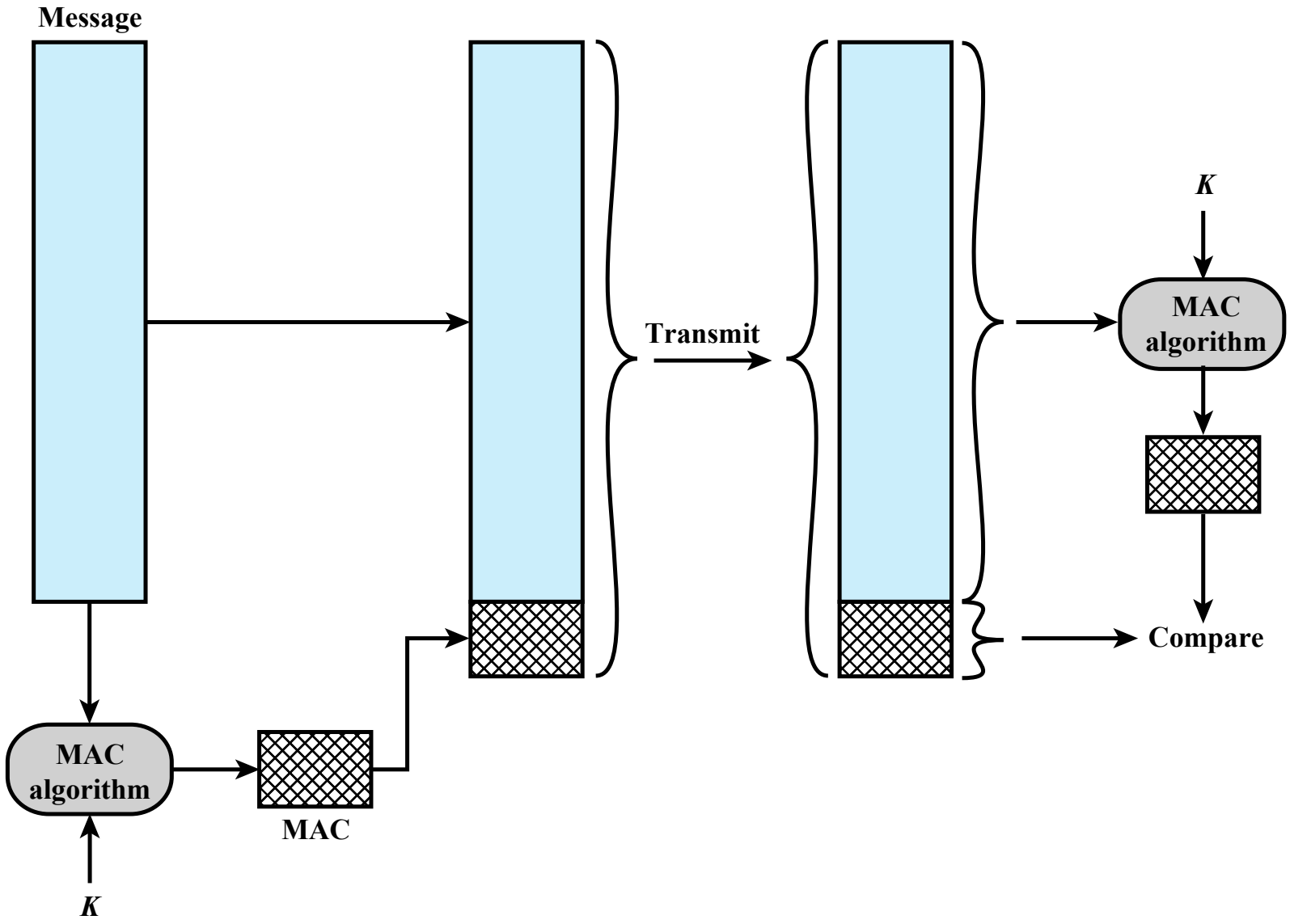


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Hash Functions

- condenses arbitrary message to fixed size
- h = H(M)
- No secret key needed
- usually assume hash function is public
- hash used to detect changes to message
- E.g SHA (secure hash algorithm)

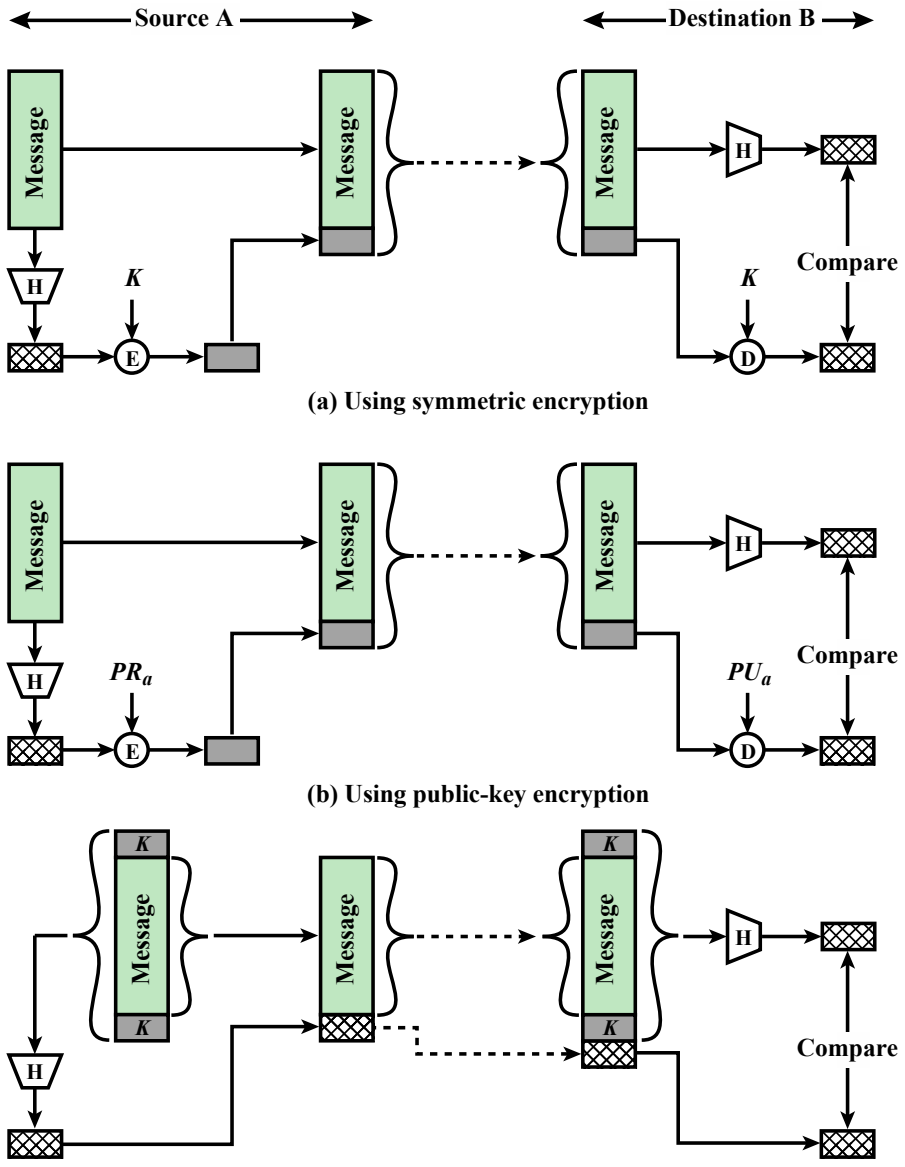


Figure 2.5 Message Authentication Using a One-Way Hash Function.

Hash Function Requirements

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find $y \neq x$ such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Security of Hash Functions

There are two approaches to attacking a secure hash function:

- **Cryptanalysis**
  - Exploit logical weaknesses in the algorithm
- **Brute-force attack**
  - Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm

Additional secure hash function applications:

- **Passwords**
  - Hash of a password is stored by an operating system
- **Intrusion detection**
  - Store H(F) for each file on a system and secure the hash values

A Simple Hash Function: **RXOR rule**

- Initially set the n-bit hash value to zero.
- Divide bit stream into n-bit blocks.
- Process each successive n-bit block of data with following two steps:
  - Rotate the current hash value to the left by one bit.
  - XOR the block with previous hash value to get new hash value.
- Good for data integrity but useless for security

Public-Key Encryption Structure

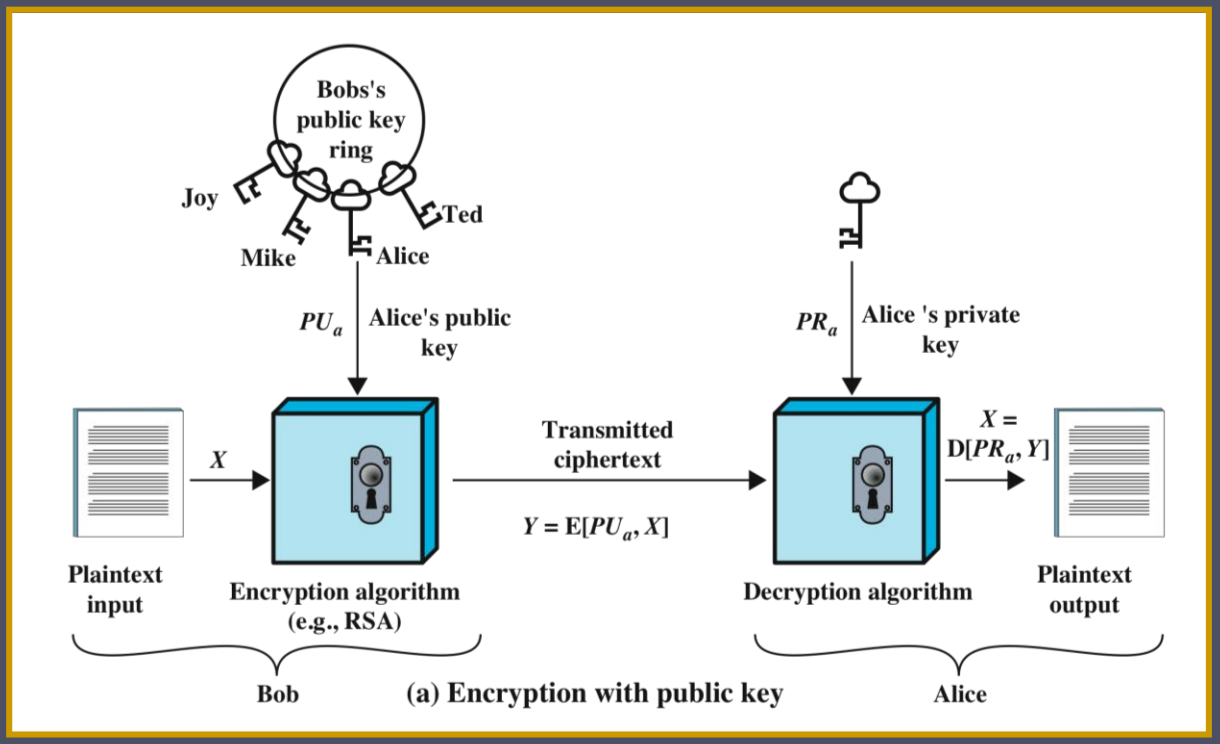
Publicly proposed by Diffie and Hellman in 1976

Asymmetric

- Uses pair of keys
- Public key and private key
- Public key is made public for others to use

Any of the keys can be used for encryption, the other key is required for decryption

complements rather than replaces private key cryptography



Secrecy mode of operation

- **Plaintext**
  - Readable message or data that is fed into the algorithm as input
- **Encryption algorithm**
  - Performs transformations on the plaintext
- **Public and private key**
  - Pair of keys, one for encryption, one for decryption
- **Ciphertext**
  - Scrambled message produced as output
- **Decryption key**
  - Produces the original plaintext

Secrecy Mode of Operation

1. If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
2. When Alice receives the message, she decrypts it using her private key.

- No other recipient can decrypt the message because only Alice knows Alice's private key.

Authenticity mode of operation

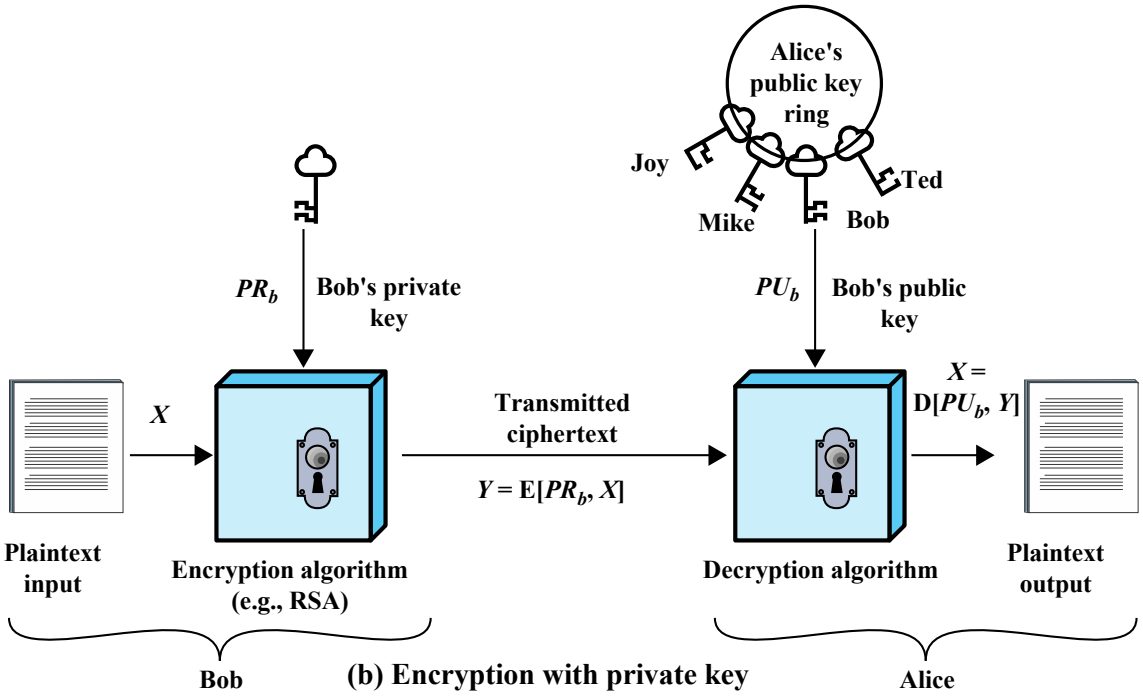


Figure 2.6 Public-Key Cryptography

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

Essential Steps Public-Key Cryptography

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file.
   - This is the public key. As previous Figure suggests the companion key is kept private.
   - Each user maintains a collection of public keys obtained from others.

Symmetric vs Public-Key

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Table 2.3

Applications for Public-Key Cryptosystems

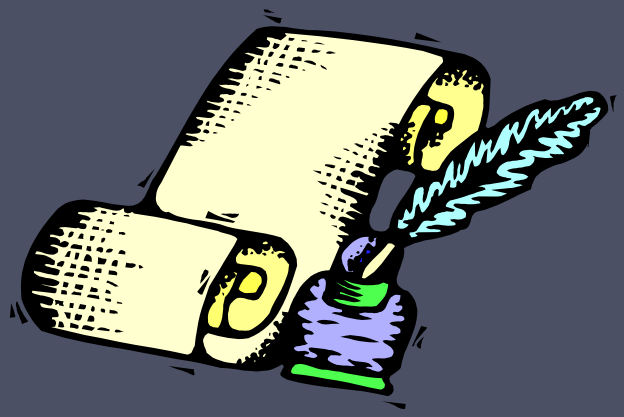
Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977	Most widely accepted and implemented approach to public-key encryption	Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
Diffie-Hellman key exchange algorithm	Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages	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		

Digital Signatures

- Used for authenticating both source and data integrity
- Created by encrypting hash code with private key
- Does not provide confidentiality
  - Even in the case of complete encryption
  - Message is safe from alteration but not eavesdropping



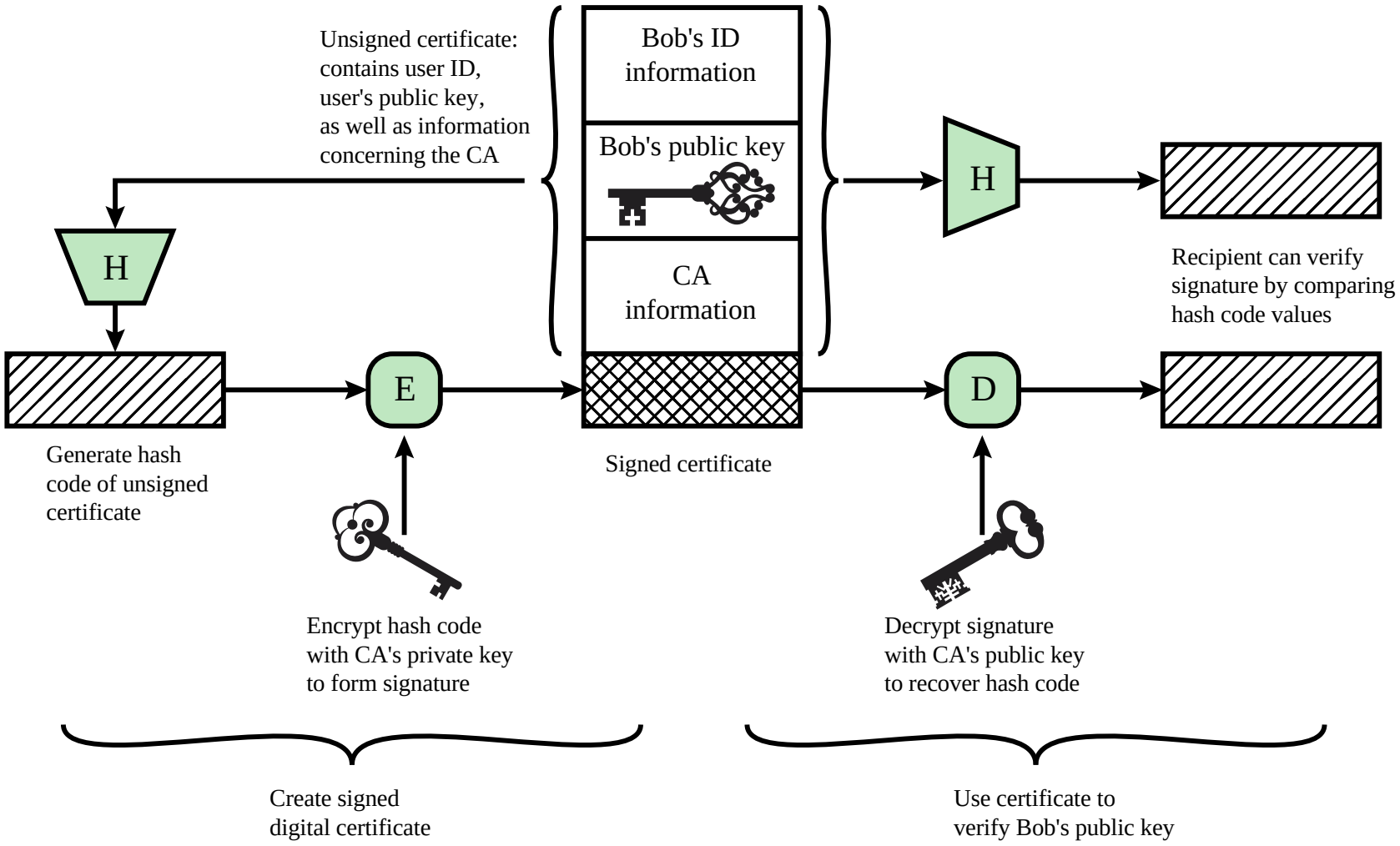
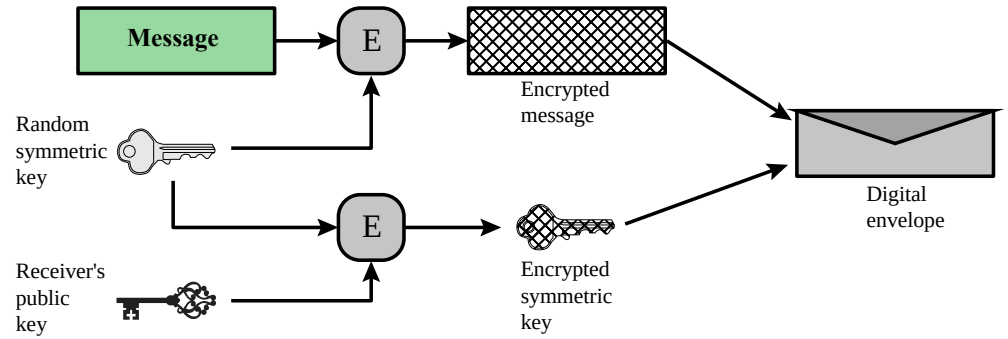


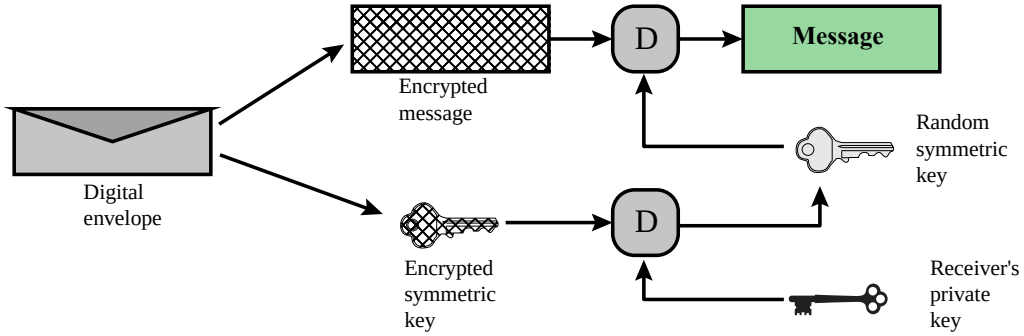
Figure 2.7 Public-Key Certificate Use

Digital Envelopes

- Protects a message without needing to first arrange for sender and receiver to have the same secret key
- Equates to the same thing as a sealed envelope containing an unsigned letter



(a) Creation of a digital envelope



(b) Opening a digital envelope

Figure 2.8 Digital Envelopes

Summary

- Confidentiality with symmetric encryption
  - Symmetric encryption
  - Symmetric block encryption algorithms
  - Stream ciphers
- Message authentication and hash functions
  - Authentication using symmetric encryption
  - Message authentication without message encryption
  - Secure hash functions
  - Other applications of hash functions

- Public-key encryption
  - Structure
  - Applications for public-key cryptosystems
  - Requirements for public-key cryptography
  - Asymmetric encryption algorithms
- Digital signatures and key management
  - Digital signature
  - Public-key certificates
  - Symmetric key exchange using public-key encryption
  - Digital envelopes