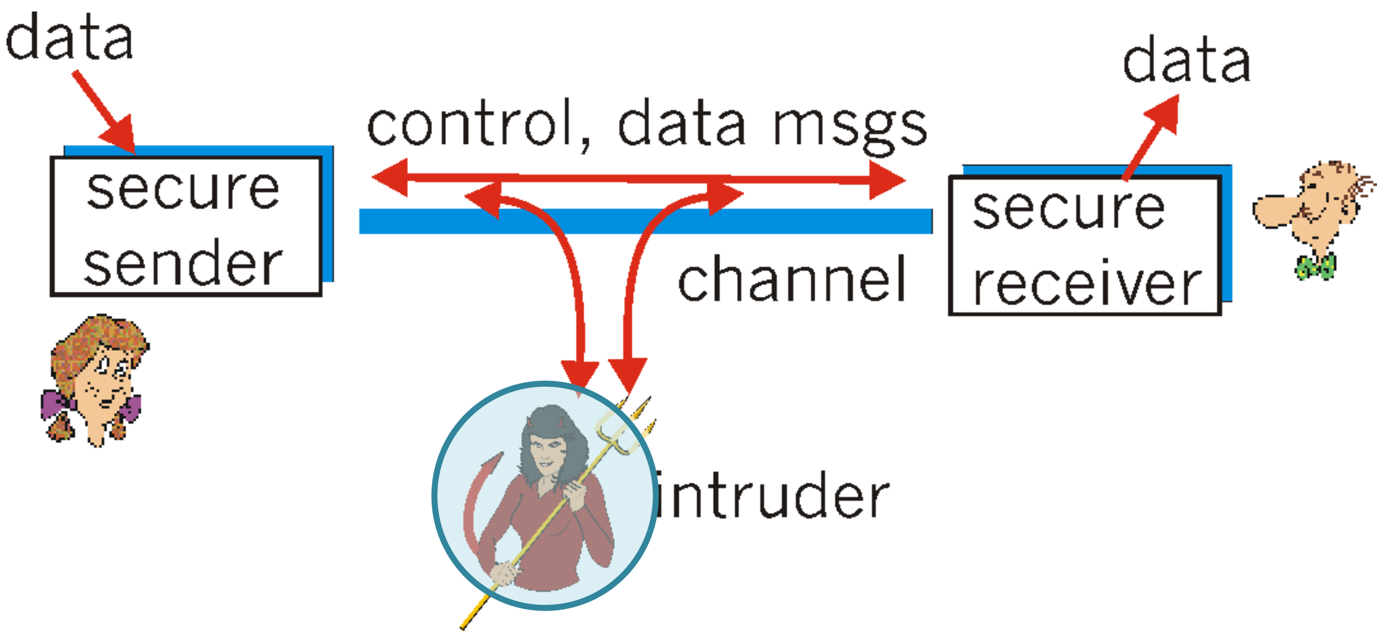
CS321: Computer Networks

Security in Computer Networks

Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Jodhpur
E-mail: manaskhatua@iitj.ac.in

Introduction

- information is an asset that has a value like any other asset
- information needs to be secured from attacks



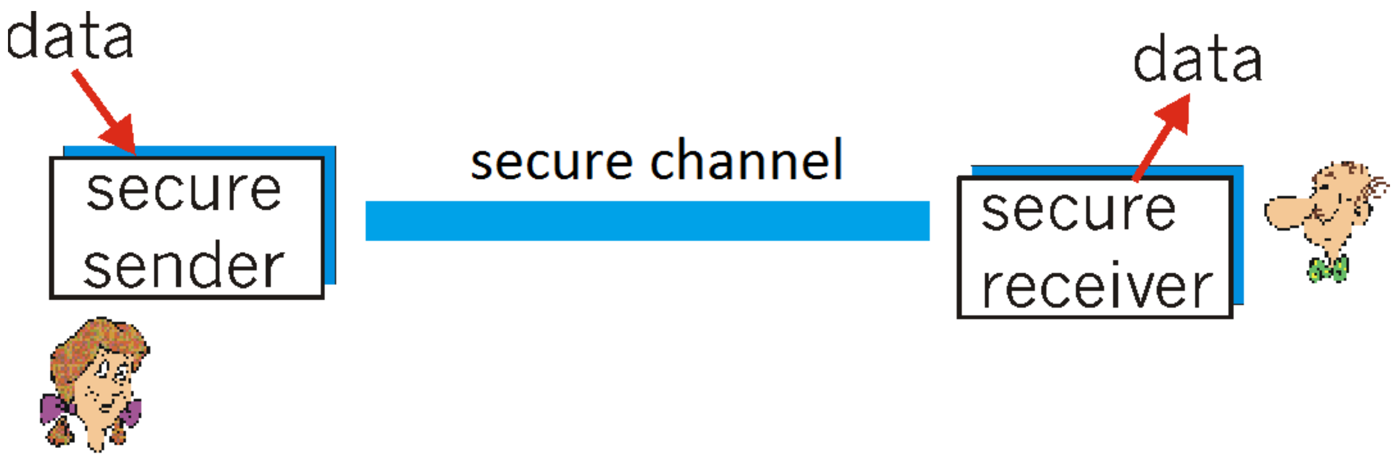
Security Goals

Confidentiality

Message integrity

End point authentication

Operational security

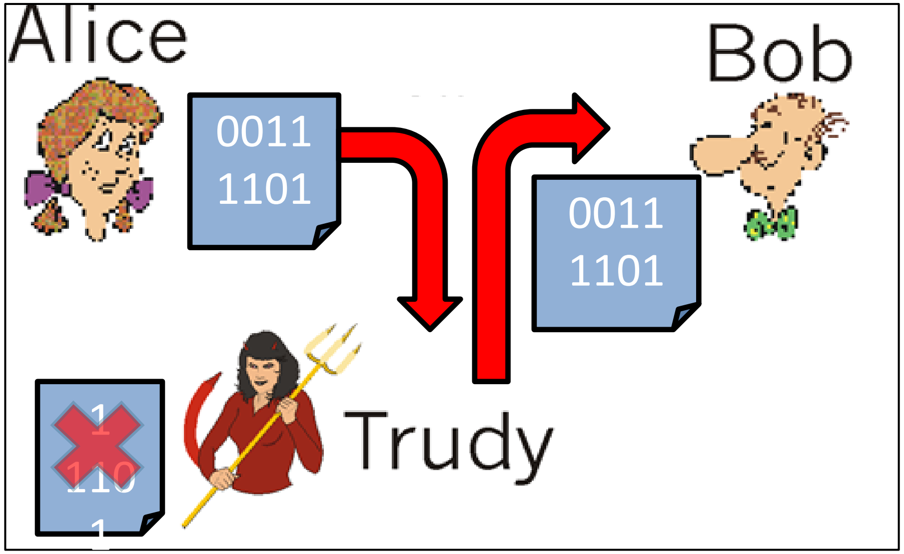


Cont…

Confidentiality | Message integrity | End point authentication | Operational security

- Information needs to be hidden from unauthorized access

- Only the sender and intended receiver should be able to understand the contents of the transmitted message
- How?
  - Using Encryption

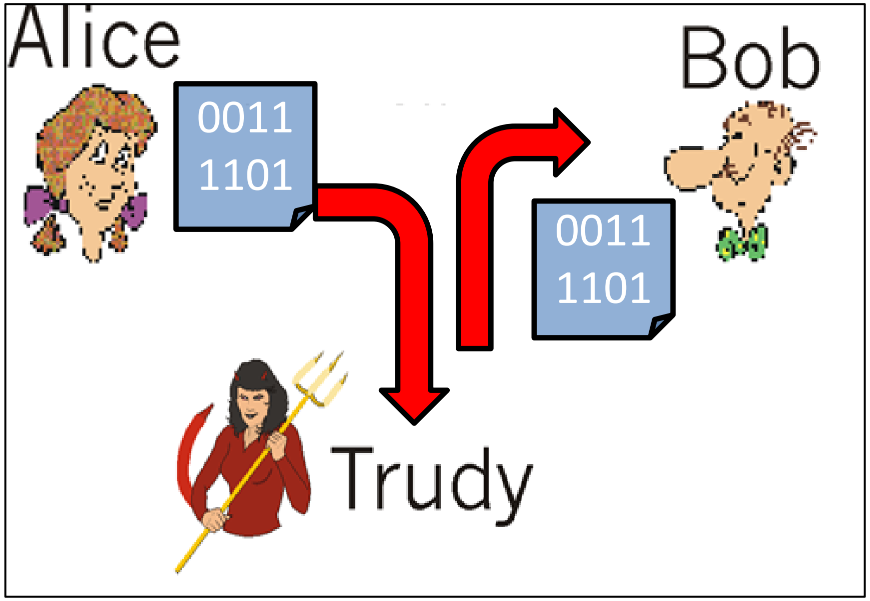


Cont...

Confidentiality | Message integrity | End point authentication | Operational security

- Message is protected from unauthorized change

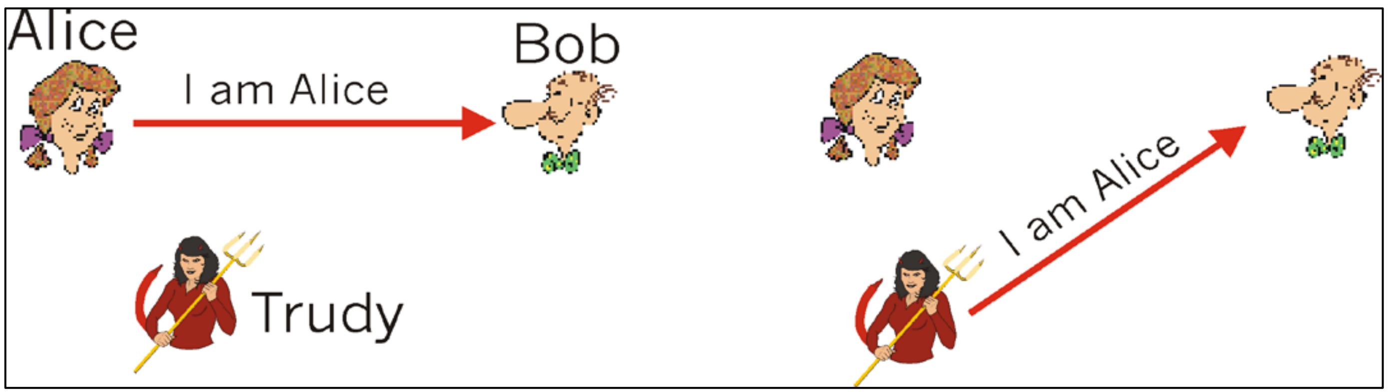
- Alice and Bob want to ensure that the content of their communication is not altered, either maliciously or by accident, in transit.
- How?
  - Using extensions of checksumming techniques



Cont…

Confidentiality | Message integrity | **End point authentication** | Operational security

- Transaction is protected from unauthorized access



- Both the sender and receiver should be able to confirm the identity of the other party involved in the communication
- How?
  - Using user authentication mechanism

Cont…

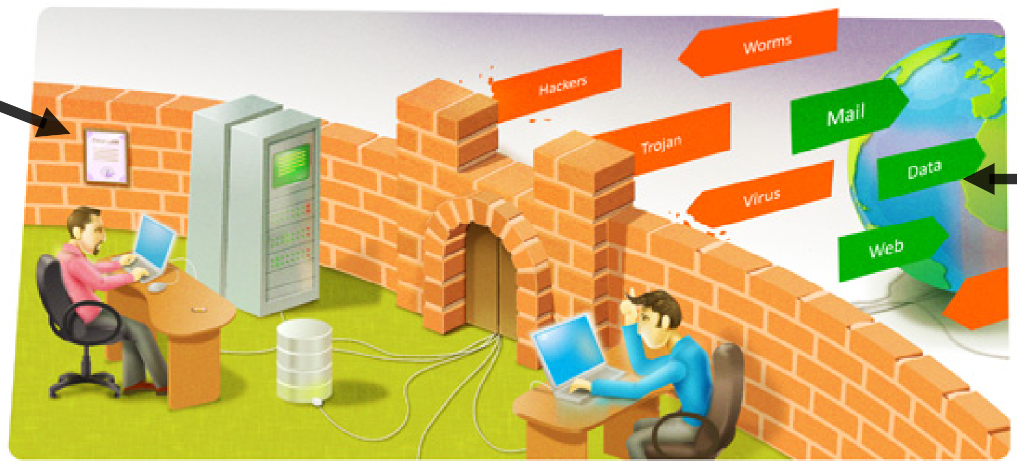
Confidentiality

Message integrity

End point authentication

Operational security

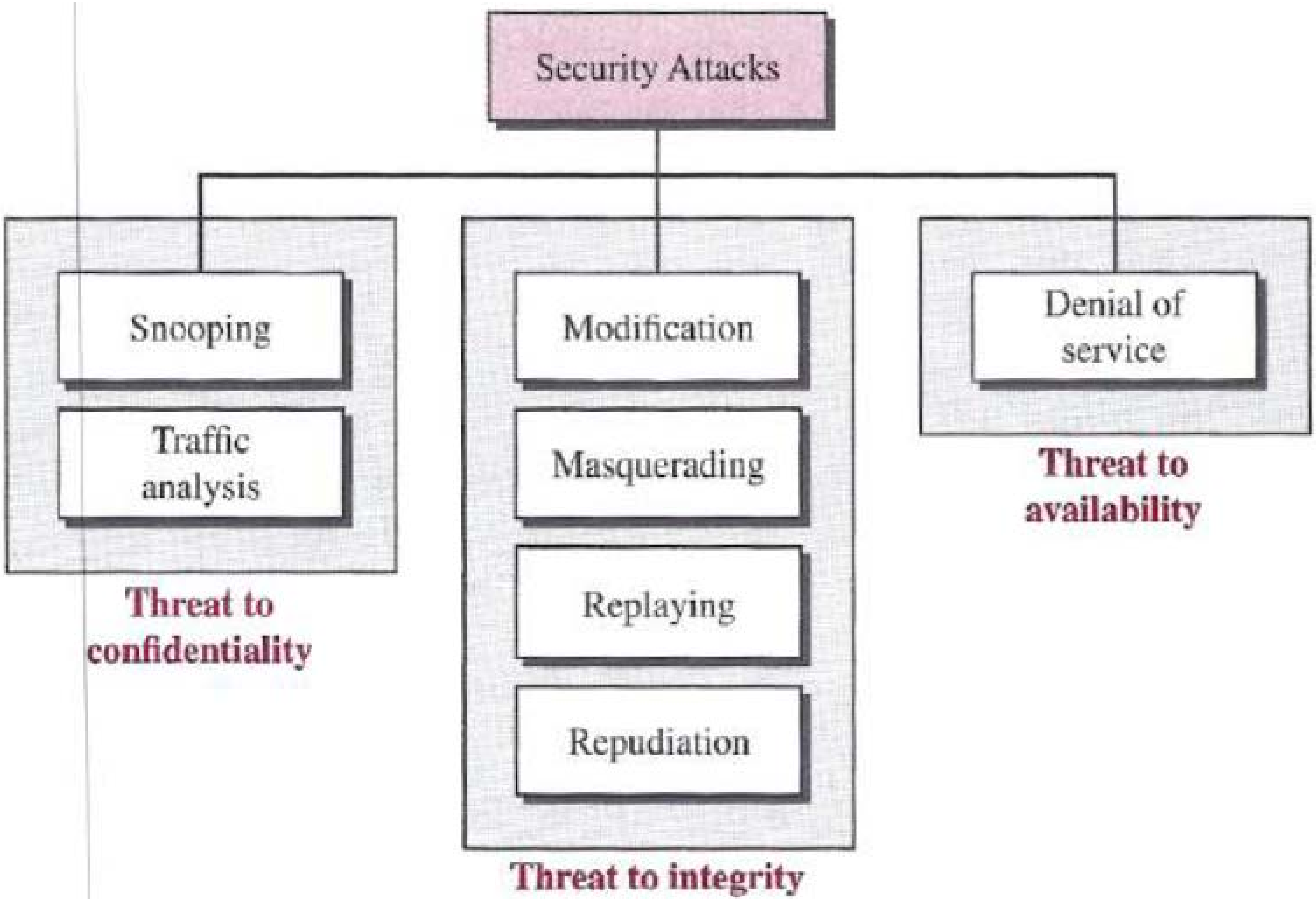
Firewall



Viruses from Public network

- Application needs to be properly operational
- How?
  - Using Firewall and IDS (Intrusion Detection System)

Security Attacks



Cont…

- *Snooping :* unauthorized access to or interception of data.
- *Traffic Analysis :* obtain some other types of information by monitoring online traffic.

- *Modification :* modifies the information to make it beneficial to the attacker
- *Masquerading* or *spoofing* : the attacker impersonates somebody else.

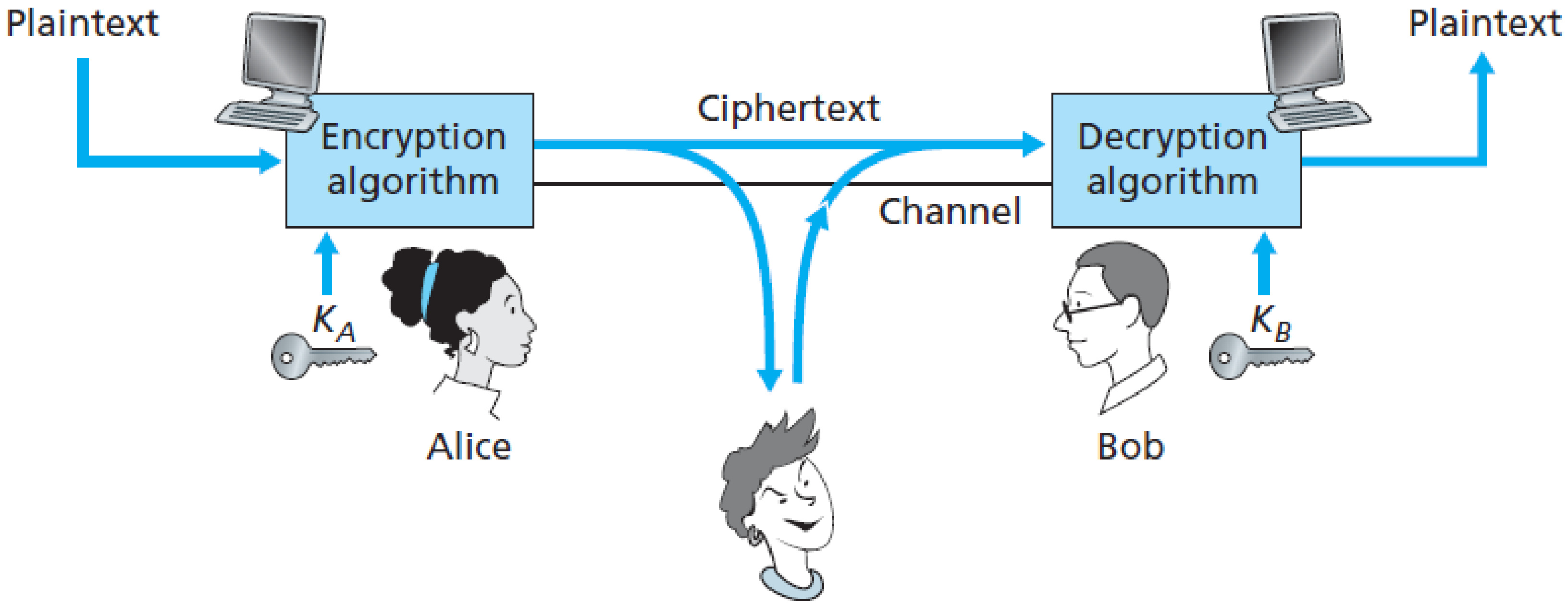
- *Replaying :* the attacker obtains a copy of a message sent by a user and later tries to replay it.
- *Repudiation :* The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

- *Denial of Service :* It may slow down or totally interrupt the service of a system.

Principles of Cryptography

- It has a long history dating back at least as far as Julius Caesar.

- Cryptographic techniques allow a sender to disguise data so that an intruder can gain no information from the intercepted data.



Cont…

- To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a key
- To create the plaintext from ciphertext, Bob uses a decryption algorithm and a key
- Based on type of key
  - symmetric key systems : Alice's and Bob's keys are identical and are secret
  - public key systems : a pair of keys is used. One of the keys is known to both Bob and Alice (indeed, it is known to the whole world). The other key is known only by either Bob or Alice (but not both).

Symmetric Key Cryptography

Symmetric-key Ciphers

- We refer to encryption and decryption algorithms as *ciphers*.
- A *key* is a set of values (numbers) that the cipher operates on.
- It needs secure key exchange mechanism.

Caesar Cipher

- Substitute each letter by a letter *k* index away (allowing wraparound; that is, having the letter z followed by the letter a)

```
 plaintext: abcd efgh ijkl mnop qrst uvwx yz
ciphertext: defg hijk lmno pqrs tuvw xyza bc
```

K=3

Plaintext: bob, i love you. alice

Ciphertext: ere, l oryh brx. dolfh

Remark: only 25 possible values for *k*, easy to break

Monoalphabetic Cipher

- *Main Idea*: Rather than substituting according to a regular pattern (for example, substitution with an offset of k for all letters), any letter can be substituted for any other letter, as long as each letter has a unique substitute letter, and vice versa.

Plaintext letter:	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 letter:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

Plaintext: bob, i love you. alice

Ciphertext: nkn, s gktc wky. mgsbc

Remark: 26! (on the order of 10^{26}) possible pairings

Cont…

- A brute-force approach of trying all 10^{26} possible pairings would require far too much work to be a feasible way of breaking the encryption algorithm and decoding the message.

- But, using statistical analysis of the plaintext language, it becomes relatively easy to break this code !
  - the letters *e* and *t* are the most frequently occurring letters in typical English text
  - particular two- and three-letter occurrences of letters appear quite often together (for example, “in,” “it,” “the,” “ion,” “ing,” and so forth)
- By guessing few words related to contextual information
  - For example, if Trudy the intruder is Bob’s wife and suspects Bob of having an affair with Alice, then she might suspect that the names “bob” and “alice” appear in the text.

Polyalphabltic Ciphers

- *Main Idea*: It uses multiple monoalphabetic ciphers, with a specific monoalphabetic cipher to encode a letter in a specific position in the plaintext message.

Plaintext letter:	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
$C_1(k = 5)$:	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
$C_2(k = 19)$:	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

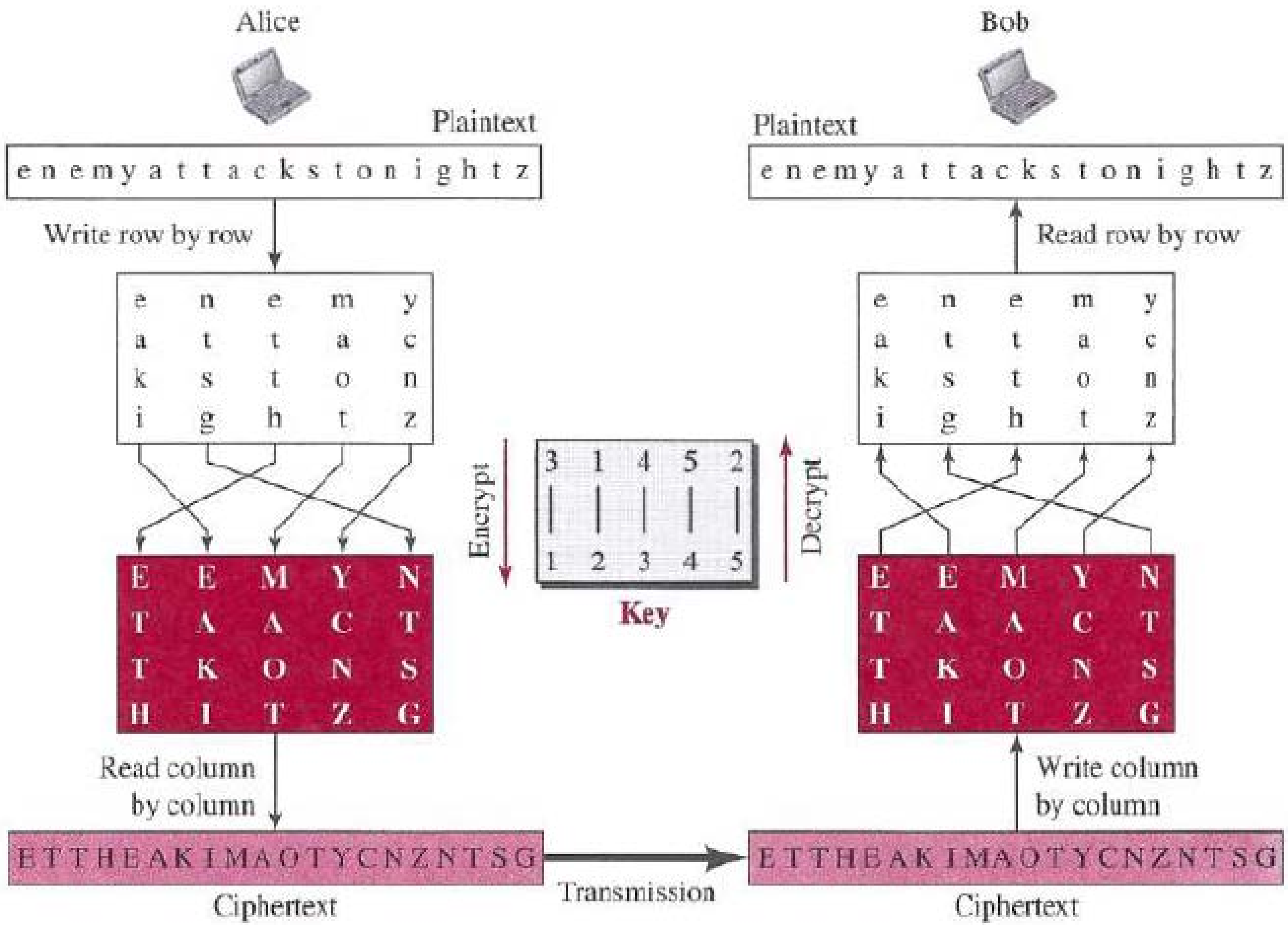
- We might choose to use these two Caesar ciphers, C1 and C2, in the repeating pattern C1, C2, C2, C1, C2.

Plaintext: bob, i love you.

Ciphertext: ghu, n etox dhz.

Transposition Ciphers

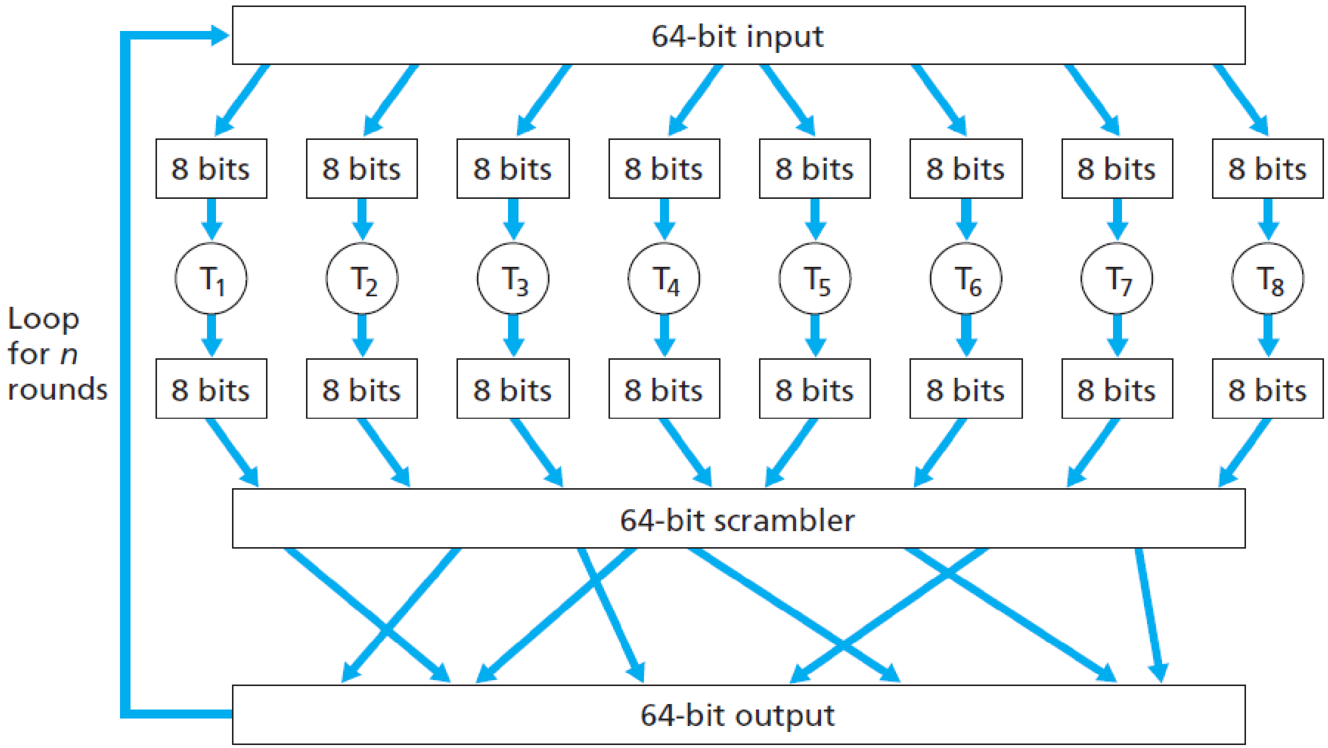
- *Main Idea*: It does not substitute one symbol for another; instead it changes the location of the symbols.



Ciphers in Modern times

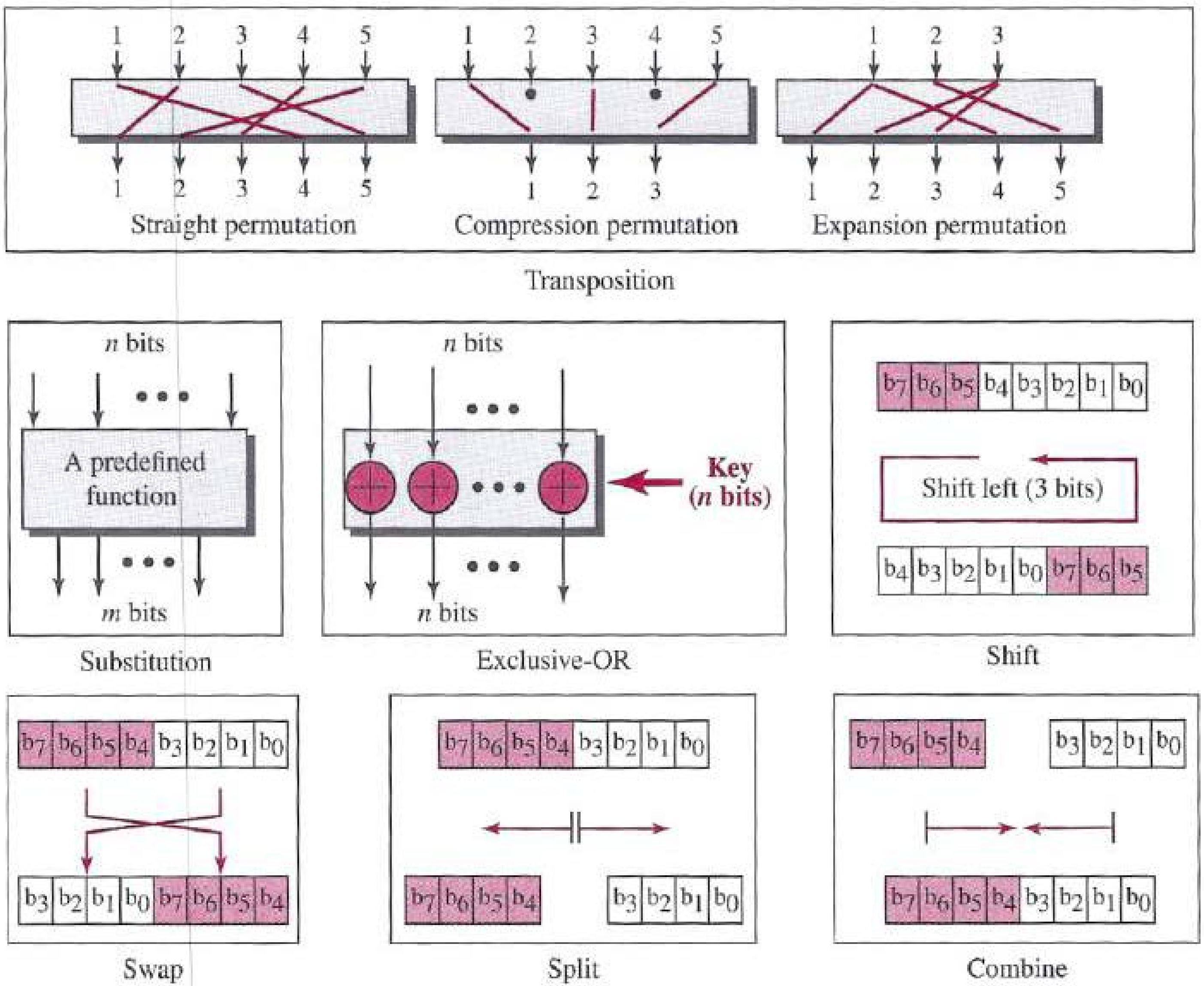
- Two broad classes of symmetric-key encryption:
  - stream ciphers
    - where plaintext digits are combined with a pseudorandom cipher digit stream (keystream)
    - used in Wireless LANs
    - E.g., RC4 (Rivest Cipher 4)
  - block ciphers
    - operates on large blocks of digits with a fixed, unvarying transformation
    - used in many secure Internet protocols, including PGP (for secure e-mail), SSL (for securing TCP connections), and IPsec (for securing the network-layer transport).
    - E.g., DES (Data Encryption Standard),
      AES (Advanced Encryption Standard)

Block Cipher



- the message to be encrypted is processed in blocks of *k* bits.
- typically use functions that simulate randomly permuted tables
- Each 8-bit chunk is processed by an 8-bit to 8-bit table

Cont…


Straight permutation
Compression permutation
Expansion permutation
Transposition
n bits
A predefined function
m bits
Substitution
n bits
Key (n bits)
n bits
Exclusive-OR
Shift left (3 bits)
Shift
Swap
Split
Combine

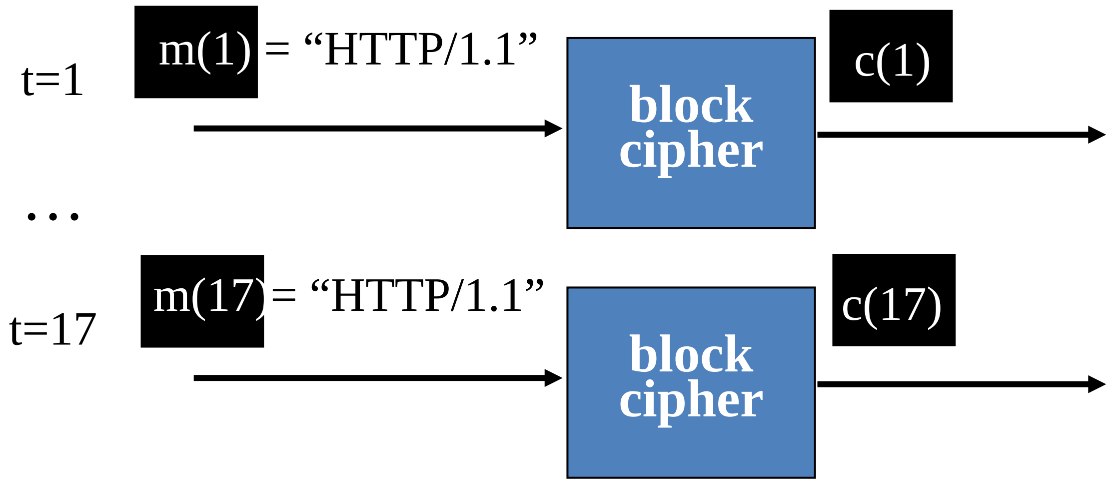
Cont…

- Popular block ciphers:
  - DES (Data Encryption Standard),
  - AES (Advanced Encryption Standard),

- DES uses 64-bit blocks with a 56-bit key
- AES uses 128-bit blocks and can operate with keys that are 128, 192, and 256 bits long.

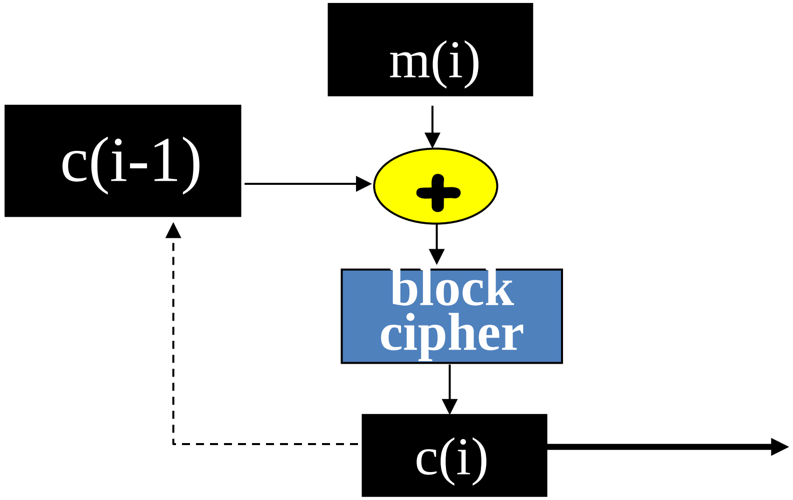
- NIST estimates that a machine that could crack 56-bit DES in one second (that is, try all 2^{56} keys in one second) would take approximately 149 trillion years to crack a 128-bit AES key.

Cipher-Block Chaining

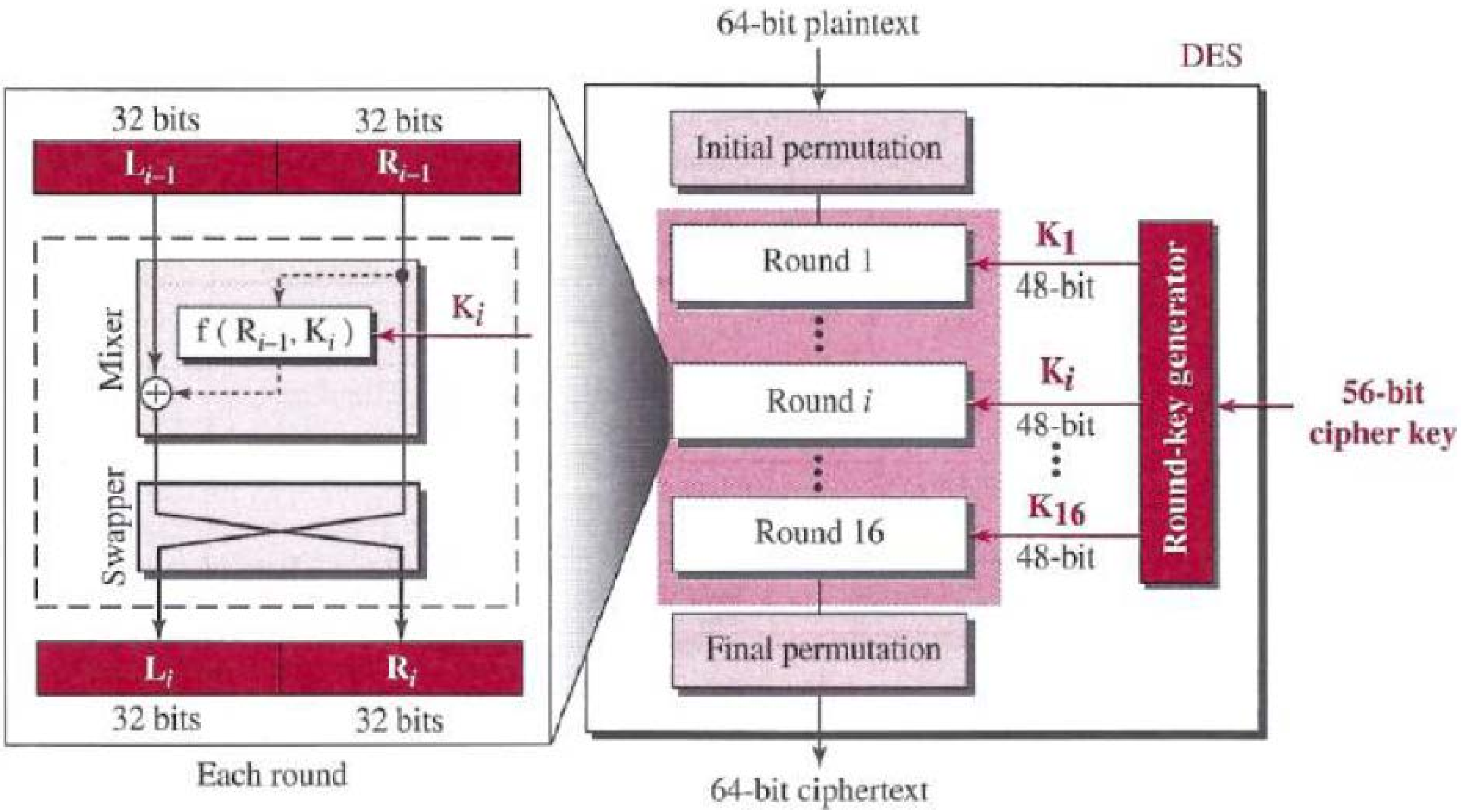


- *Drawback:* if input block is repeated, this coding will produce same cipher text

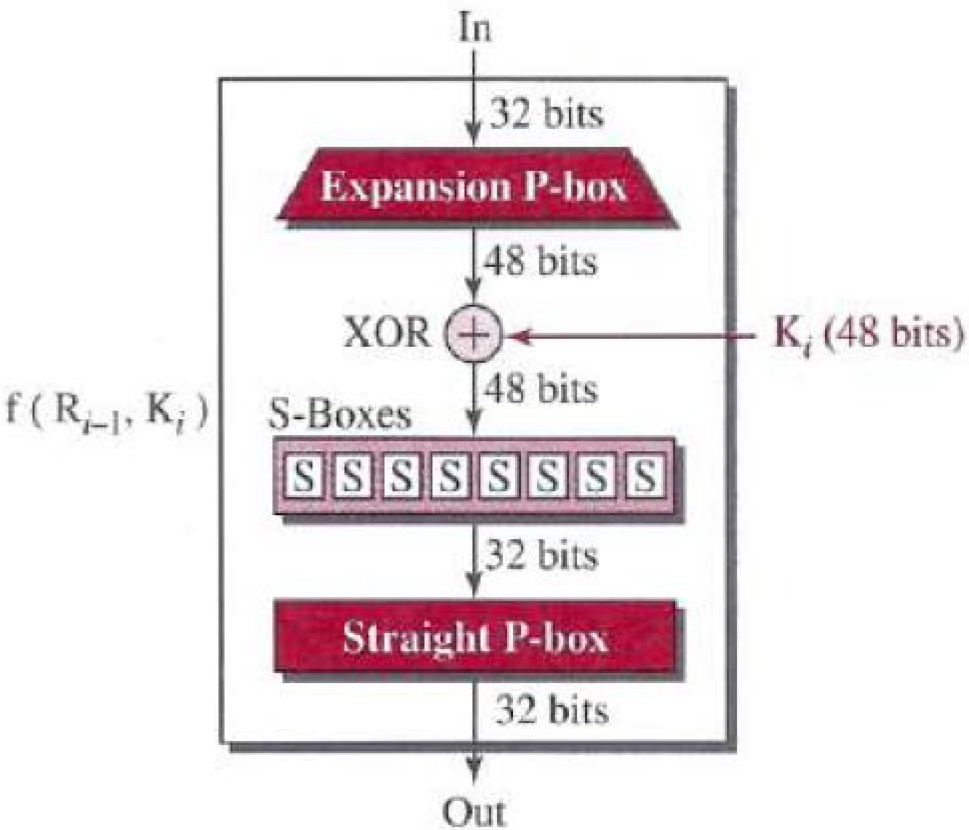
- Solution: Cipher Block Chaining
  - XOR i^{th} input block, m(i), with previous block of cipher text, c(i-1)



Data Encryption Standard (DES)



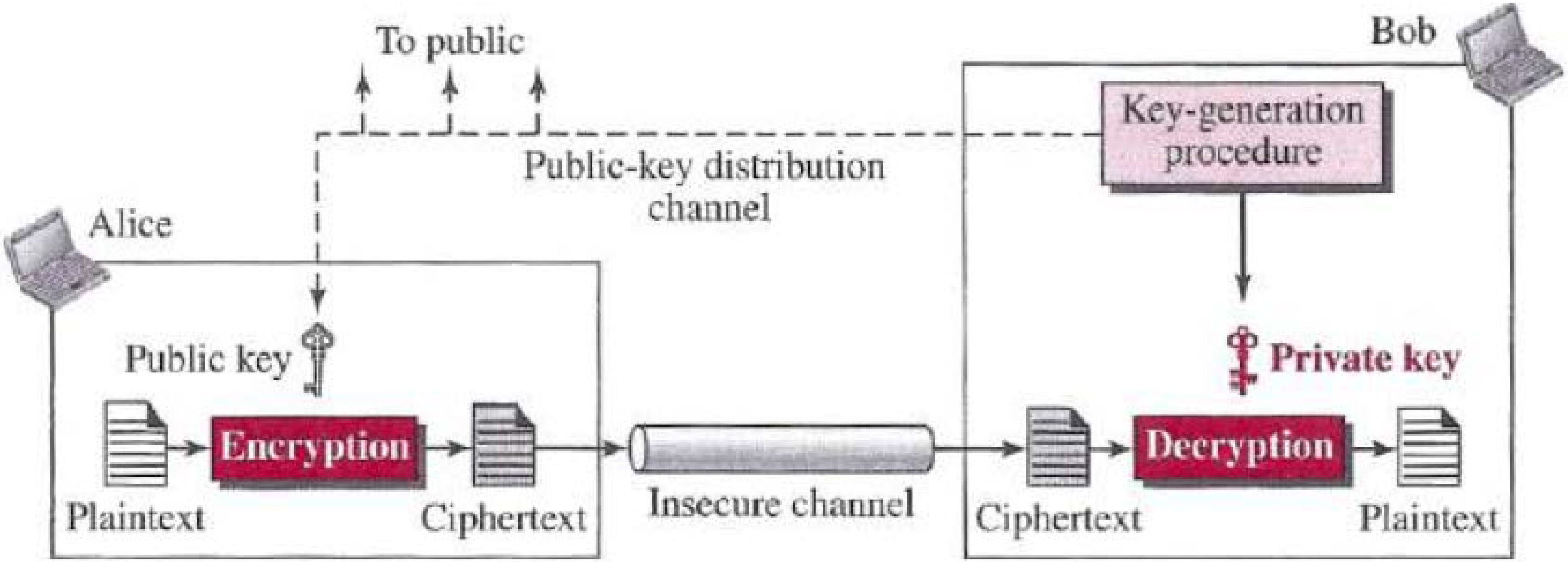
Cont...



- DES takes a 64-bit plaintext and creates a 64-bit ciphertext;
- The same 56-bit cipher key is used for both encryption and decryption
- DES uses 16 rounds
- The heart of DES is the DES function.
- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

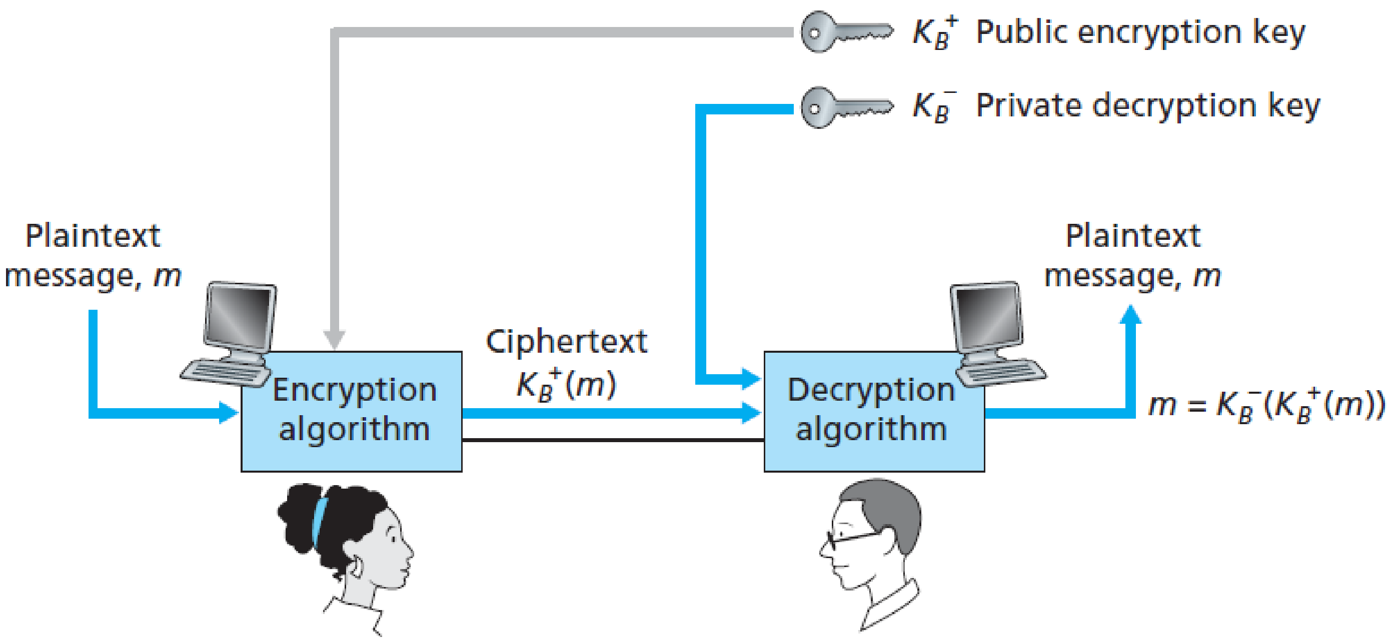
Public Key Cryptography

Public-Key Cryptography



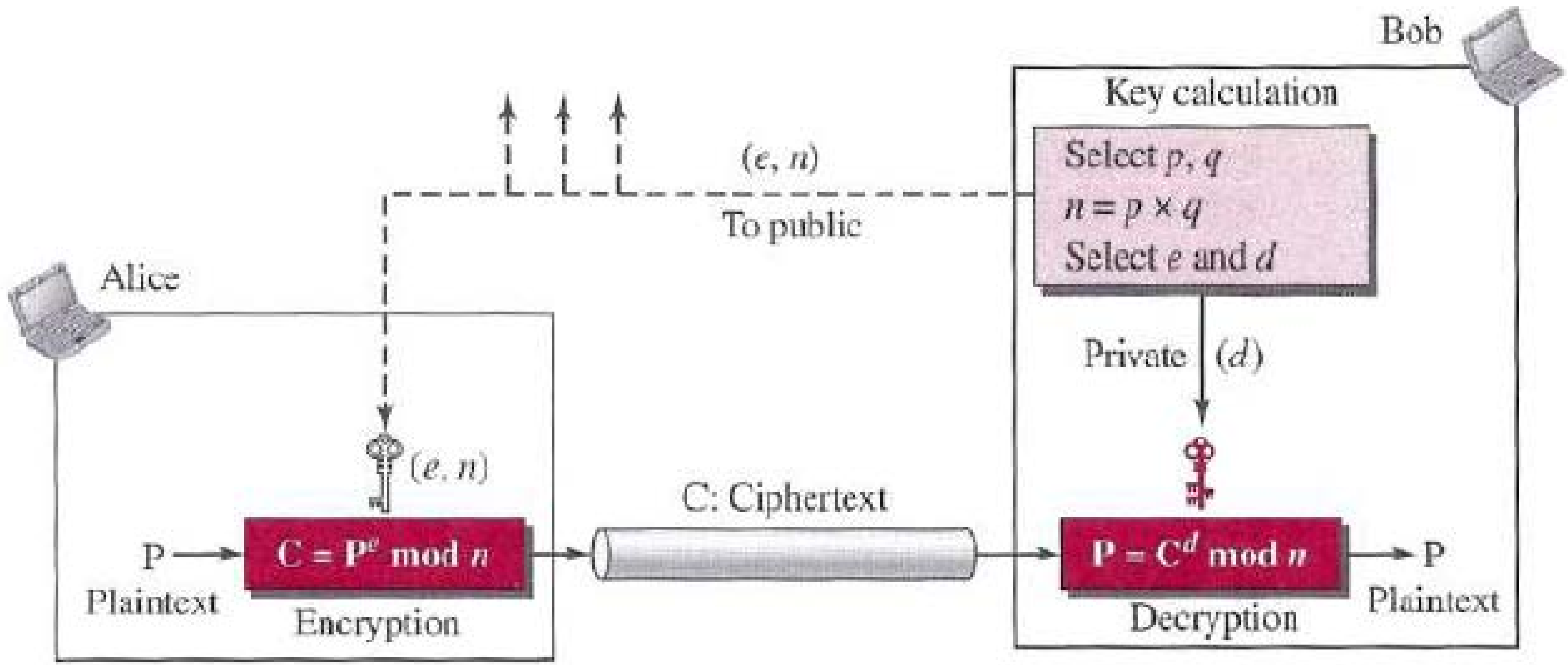
- Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on personal secrecy.
- In symmetric-key cryptography, symbols are permuted or substituted; in asymmetric-key cryptography, numbers are manipulated.

Cont…



- Two concerns
  - Intruder knows Bob's public key which Alice used. Intruder can intercept the ciphertext transmitted from Alice
    - Soln: strong cipher & key
  - Since Bob's encryption key is public, anyone can send an encrypted message to Bob, including Alice or someone claiming to be Alice.
    - Soln: Digital Signature

RSA Algorithm



- RSA (Rivest, Shamir, and Adleman)
- RSA uses two exponents, *e* and *d*, where *e* is public and *d* is private
- Suppose P is the plaintext and C is the ciphertext.

  $C = P^e \bmod n$; $P = C^d \bmod n$; n is a large number

Cont…

- How can we get those *e*, *d*, *n*?
- Procedure:

  choose two large numbers, *r* and *q*, and calculates

  $n = r \times q$ and $z = (r - 1) \times (q - 1)$

  Then, selects *e* and *d* such that $(e \times d) \bmod z = 1$.

- Example:

  let Bob choose 7 and 11 as *r* and *q*.

  So, $n = 7 \times 11 = 77$; $z = 6 \times 10 = 60$

  If, he chooses e=13, then, d=37.

  Let, Alice wants to send the plaintext 5 to Bob.

  So, $C = 5^{13} \bmod 77 = 26$

  $P = 26^{37} \bmod 77 = 5$

Cont…

- Modular arithmetic:

  $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

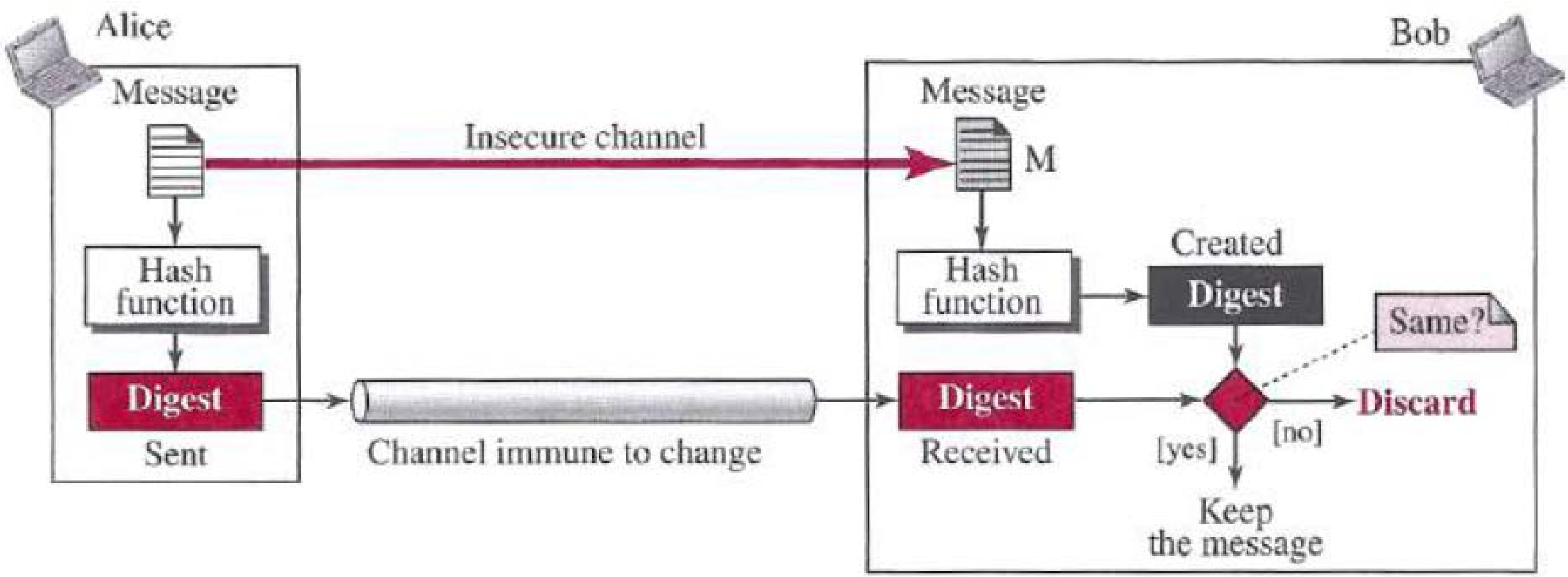
  $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

  $[(a \bmod n) \bullet (b \bmod n)] \bmod n = (a \bullet b) \bmod n$

- *Applications:*
  - useful for short messages
  - it is very slow if the message is long
  - is used in digital signatures
  - is also used for authentication

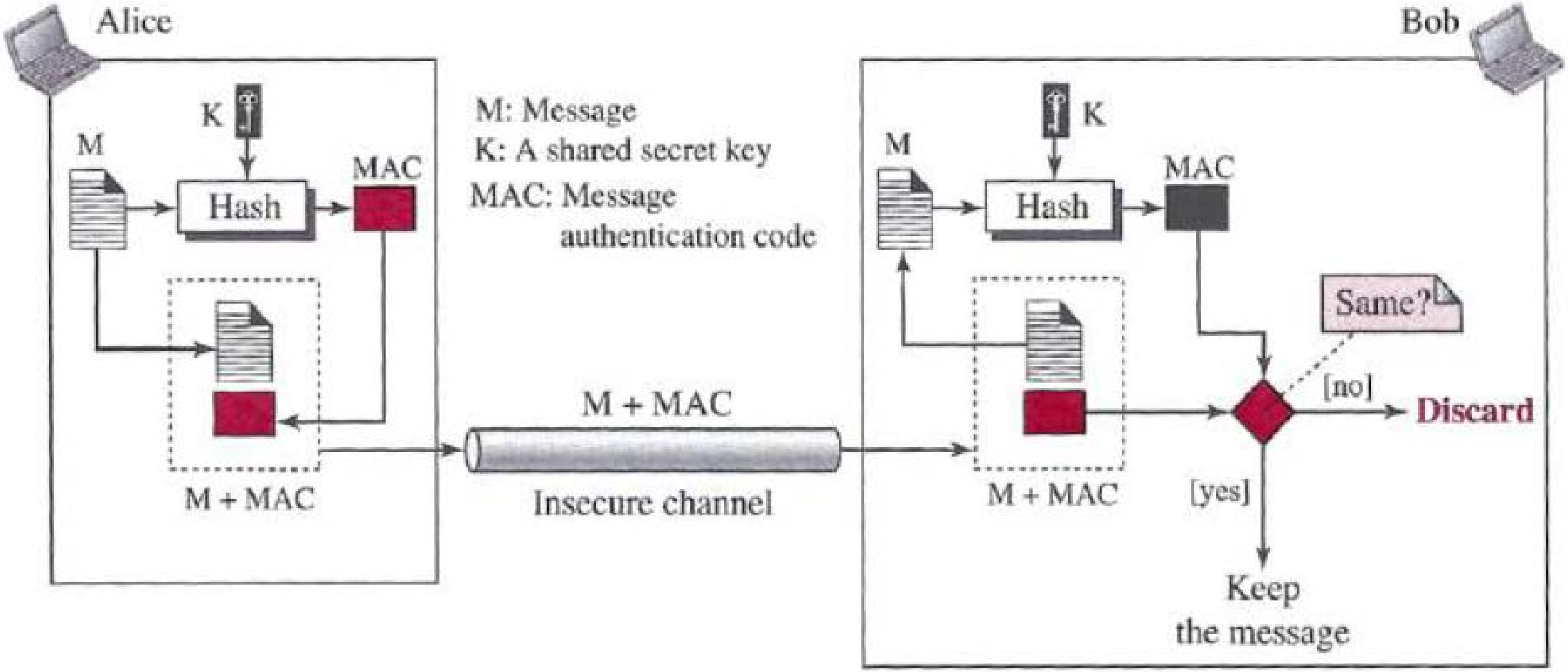
Message Integrity

- There are occasions where we may not even need secrecy but instead must have integrity: the message should remain unchanged.
- One way to preserve the integrity of a document is through the use of a *fingerprint.*
- The electronic equivalent of the document and fingerprint pair is the *message* and *digest* pair.



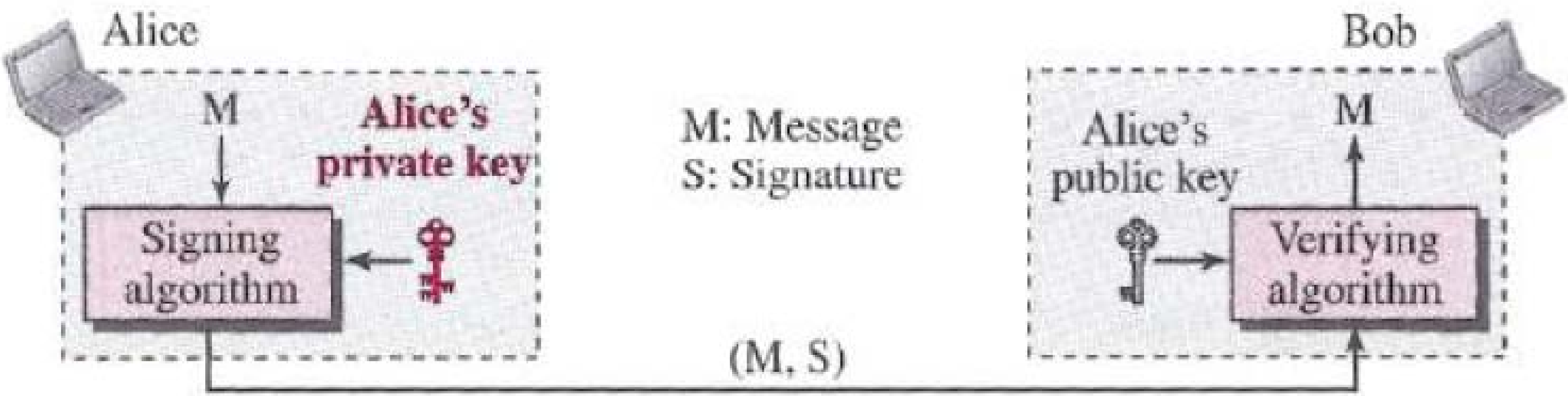
Message Authentication

- A digest can be used to check the integrity of a message
- But, to ensure the integrity of the message and the data origin authentication, we need to include a secret shared by Alice and Bob in the process.
- We achieve this by message authentication code (MAC).



Digital Signature

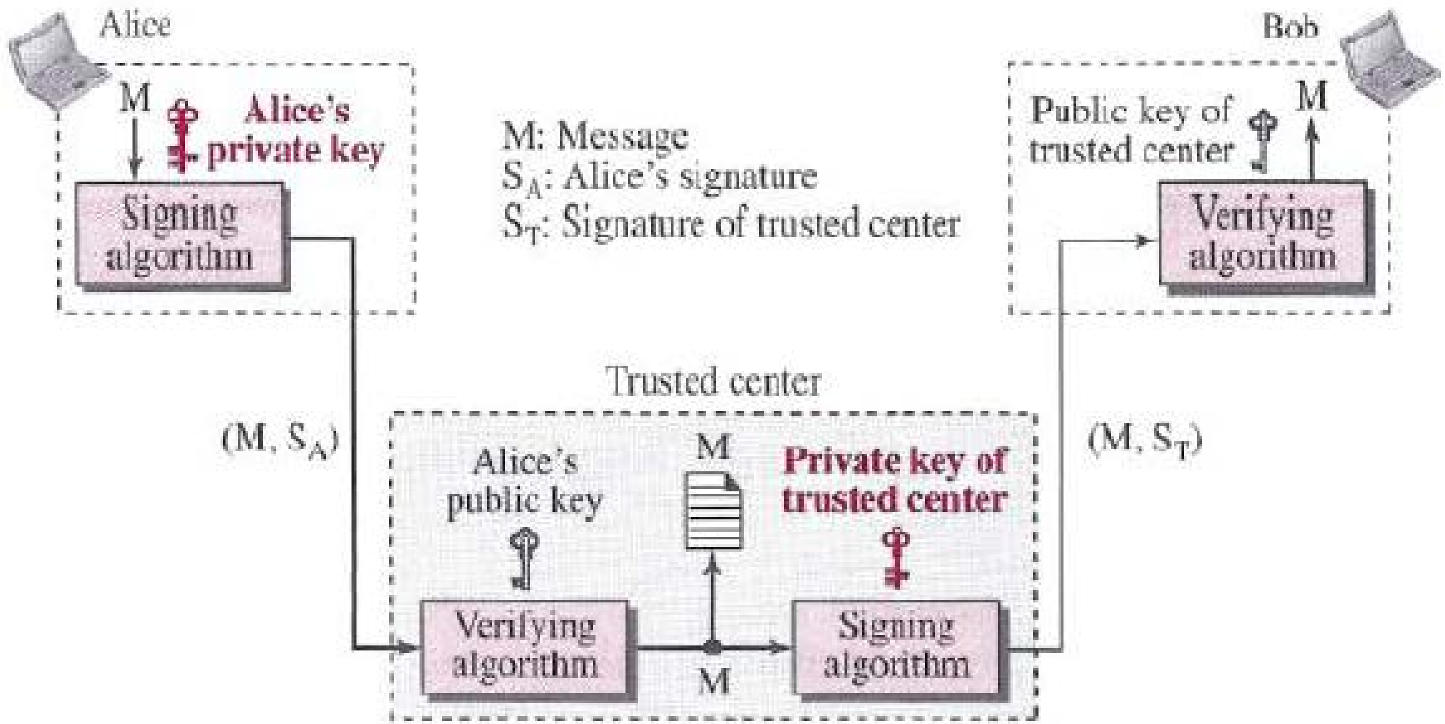
- Your signature attests to the fact that you (as opposed to someone else) have acknowledged and/or agreed with the document's contents.
- A digital signature is a cryptographic technique for achieving the same goals in a digital world.



- A cryptosystem uses the public and private keys of the receiver; a digital signature uses the private and public keys of the sender.

Trusted Centre for Nonrepudiation

- If Alice signs a message and then denies it, can Bob later prove that Alice actually signed it?
- Bob must keep the signature on file and later use Alice's public key to create the original message to prove the message in the file and the newly created message are the same.



Thanks!