



Chapter 6

Computer Network Security Basics

Objectives

- ❑ Importance of security in data communications and networking.
- ❑ Cryptography based network Security
Cryptography
- ❑ Security goal

What is network security?

- ❑ While computer systems today have some of the best security systems ever, they are more **vulnerable** than ever before.
- ❑ Network security is all about securing the communication from third party tracing, accessing, modification and likes.
- ❑ This vulnerability stems from the **world-wide access** to computer systems via the **Internet**.
- ❑ Network security is **preventing attackers** from achieving objectives through unauthorized access or unauthorized use of computers and networks.

CONT...

- ❑ Hosts attached to a network are exposed to a wider range of security threats than are unconnected hosts.
- ❑ The network provides equal access for all - **welcome** visitors as well as **unwelcome** intruders.
- ❑ **Network security** generally means providing adequate security on individual host computers, not providing security directly on the network.
- ❑ At home, you provide security for your possessions by locking your house, not by blocking the streets.

Cont...

- ❑ Once the hacker gains access to the network, four types of threat may arise:
 - Information theft
 - Identity theft
 - Data loss / manipulation
 - Disruption of service

Source of Network Intrusion

- ❑ Security threats from network intruders can come from both internal and external sources.

External Threats

- ✓ External threats arise from individuals working outside of an organization.
- ✓ They do not have authorized access to the computer systems or network.
- ✓ External attackers work their way into a network mainly from the Internet, wireless links or dialup access servers.

CONT....

- ❑ Protection from **environmental damage** such as floods, earthquakes, and heat.
- ❑ Physical security such as **locking rooms, locking down computers, keyboards**, and other devices.
- ❑ Electrical protection from power surges.
- ❑ Noise protection from placing computers away from devices that generate electromagnetic interference.

Internal Threats

- ❑ Internal threats occur when someone has **authorized** access to the network through a user **account** or have physical access to the **network equipment**.
- ❑ They often know what information is both **valuable** and **vulnerable** and how to get to it.

Basic Security Measures

❑ The basic security measures for computer systems fall into the following categories:

- | | |
|----------------------------|---|
| 1.External security | 1.Standard system attacks |
| 2.Operational security | 2.Viruses/worms and
antivirus tools |
| 3.Surveillance | 3.Firewalls |
| 4.Passwords/authentication | 4.Encryption and
Decryption Techniques |
| 5.Auditing | 5.Digital Signature |
| 6.Access rights | 6.Security Policy |

Operational Security

- Deciding **who has access to what**.
- Limiting **time of day access**.
- Limiting **day of week access**.
- Limiting **access from a location**, such as not allowing a user to use a **remote login** during certain periods or any time.

Surveillance

- ❑ Proper placement of security cameras or CCTV can deter theft and vandalism.
- ❑ Cameras can also provide a record of activities.
- ❑ Intrusion detection is a field of study in which specialists try to prevent intrusion and try to determine if a computer system has been violated.

Passwords and ID Systems

- ❑ Passwords are the most common form of security and the most abused.
- ❑ Simple rules help support safe passwords, including:
 1. **Change your password often.**
 2. **Pick a good, random password (minimum 8 characters, mixed symbols).**
 3. **Don't share passwords or write them down.**
 4. **Don't select names and familiar objects as passwords.**

Authentication

- ❑ Authentication is the process of reliably verifying the identity of someone (or something) by means of:
 - A secret (password [one-time], ...)
 - An object (smart card, ...)
 - Physical characteristics (fingerprint, retina, ...)
 - Trust

Passwords and ID Systems - Authentication?

- ❑ Many new forms of “passwords” are emerging:
 - Fingerprints
 - Face prints
 - Retina scans and iris scans
 - Voice prints
 - Ear prints

Auditing

- Creating a computer or paper audit can help **detect wrongdoing**.
- Auditing can also be used as a deterrent.
- Many network operating systems allow the administrator to **audit most types of transactions**.
- Many types of criminals have been caught because of computer-based audits.

Access Rights

- ❑ Two basic questions to access right: **who and how?**
- ❑ Who do you give access right to? No one, group of users, entire set of users?
- ❑ How does a user or group of users have access?
Read, write, delete, print, copy, execute?
- ❑ Most network operating systems have a powerful system for assigning access rights.

computer virus and a computer worm?

- ❑ Viruses are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers.
- ❑ We send e-mail document attachments, trade programs on diskettes, or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer, and so on.
- ❑ The *computer worm* is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses.

Standard System Attacks

- ☛ **Denial of service attacks**, or distributed denial of service attacks, bombard a computer site with so many messages that the site is incapable of answering valid request.
- ☛ **e-mail bombing**, a user sends an excessive amount of unwanted e-mail to someone.
- ☛ **Smurfing** is a nasty technique in which a program attacks a network by exploiting IP broadcast addressing operations.
- ☛ **Ping storm** is a condition in which the Internet Ping program is used to send a flood of packets to a server.
- ☛ **Spoofing** is when a user creates a packet that appears to be something else or from someone else.
- ☛ **Trojan Horse** is a malicious piece of code hidden inside a seemingly harmless piece of code.
- ☛ **Stealing, guessing, and intercepting** passwords is also a tried and true form of attack

Principles of Security(Security goals)

Primary Principles

- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity
- ✓ Non Repudiation

Secondary Principles

- Access Control
- Availability

Message Confidentiality:

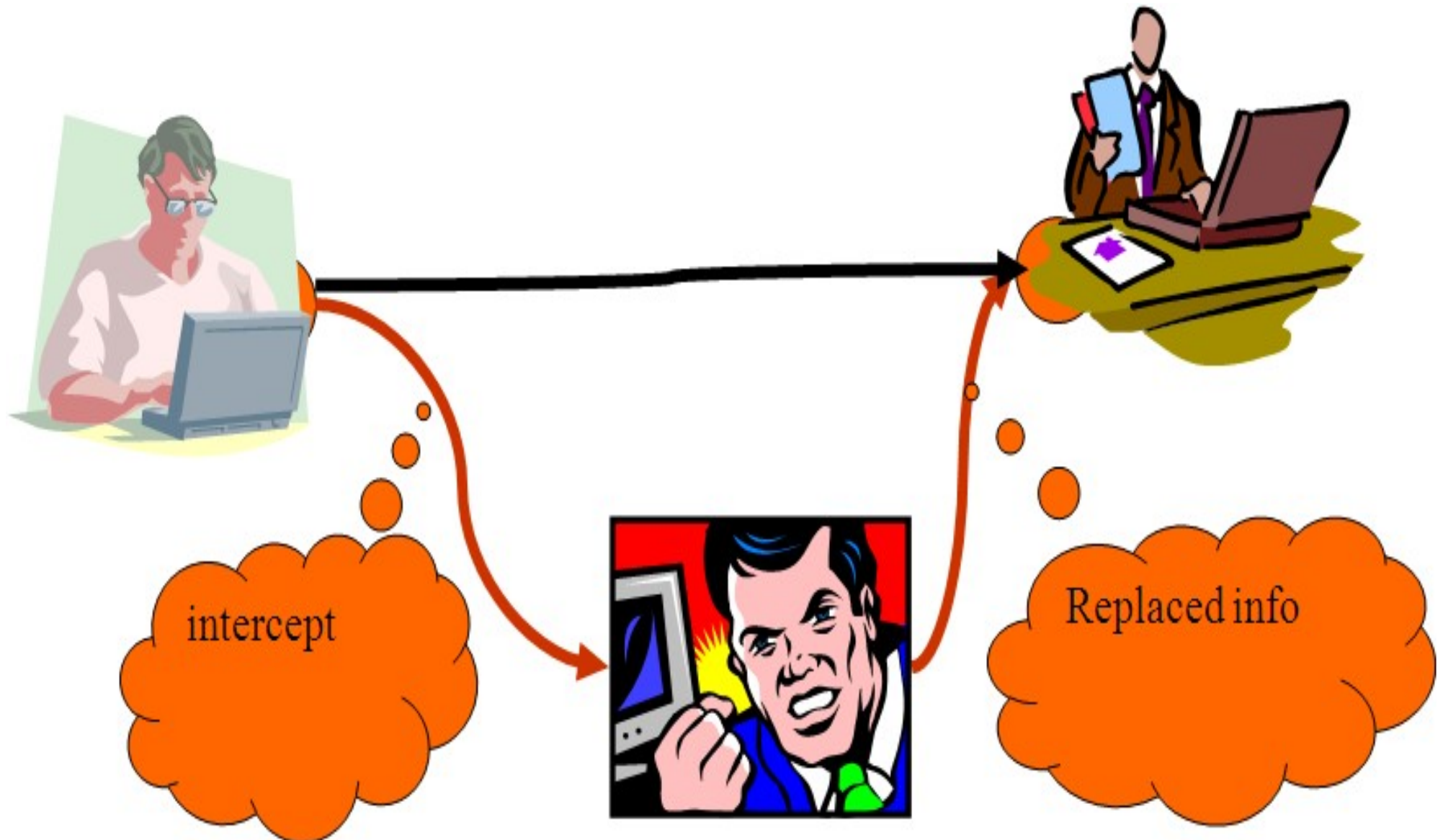
- ❑ Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- ❑ The transmitted message must make sense to only the intended receiver.
- ❑ To all others, the message must be garbage.
- ❑ When a customer communicates with her bank, He/she expects that the communication is totally confidential

Message Integrity:

- ❑ Message integrity means that the data must arrive at the receiver exactly as they were sent.
- ❑ There must be no changes during the transmission, neither accidentally nor maliciously.
- ❑ As more and more monetary exchanges occur over the Internet, integrity is crucial.
- ❑ The message must travel without any alternation.



Modification (Loss of Integrity):-

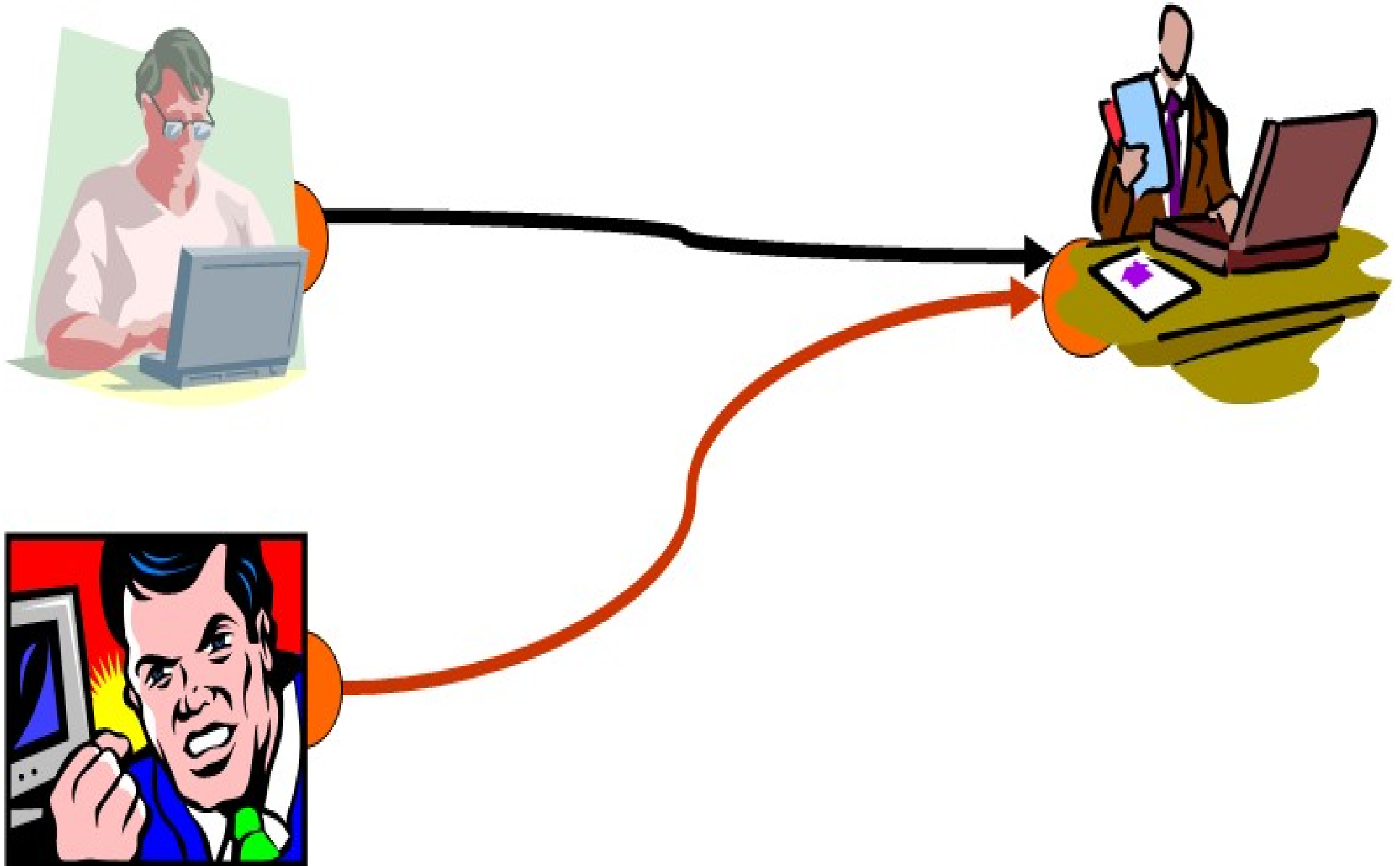


Message Authentication:

- ❑ Message authentication is a service beyond message integrity.
- ❑ In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.
- ❑ It helps in establishing proof of identities



Fabrication (Absence of Authentication)



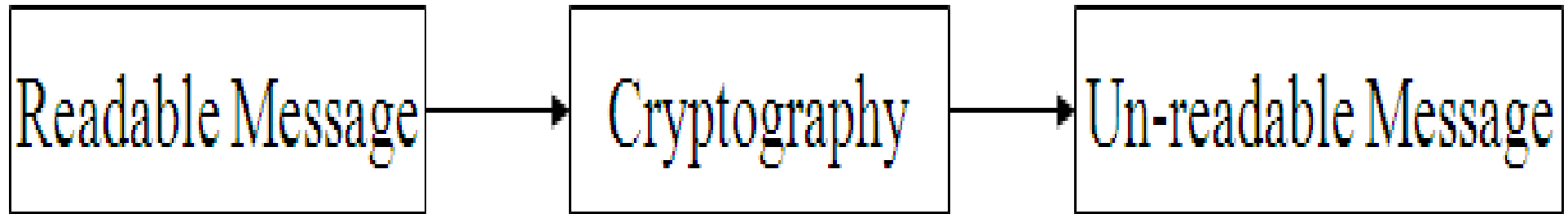
What is cryptography ?

Introduction

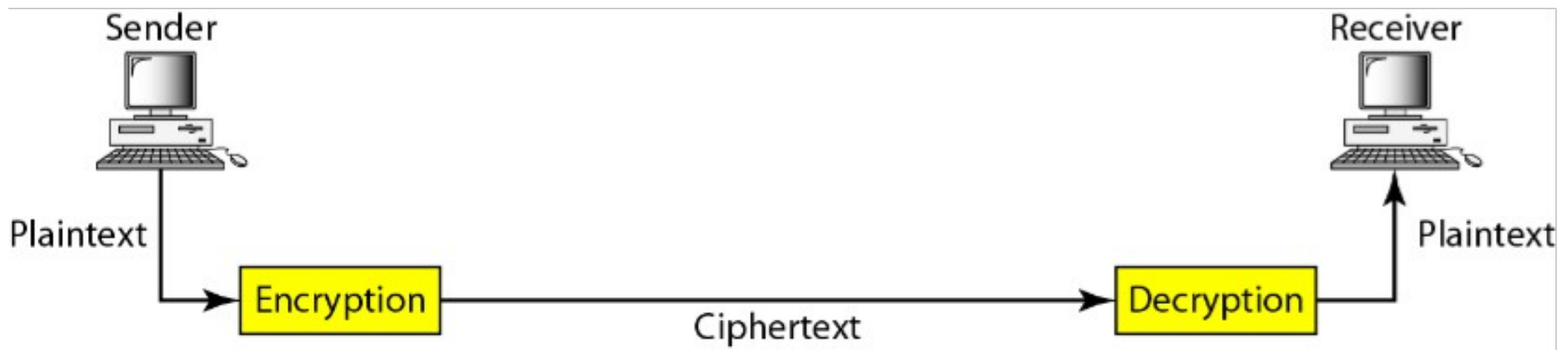
- ❑ **Cryptography** Is the science and art of transforming messages to make them secure and immune to attacks
- ❑ study of Encryption
 - Greek **kryptos** means “hidden” and **graphia** means “writings”
- ❑ **Encryption** is an ancient form of information protection. ... dates back 4,000 years.
 - process by which plaintext is converted into ciphertext.
- ❑ **Decryption** is the inverse of Encryption.

Cryptography

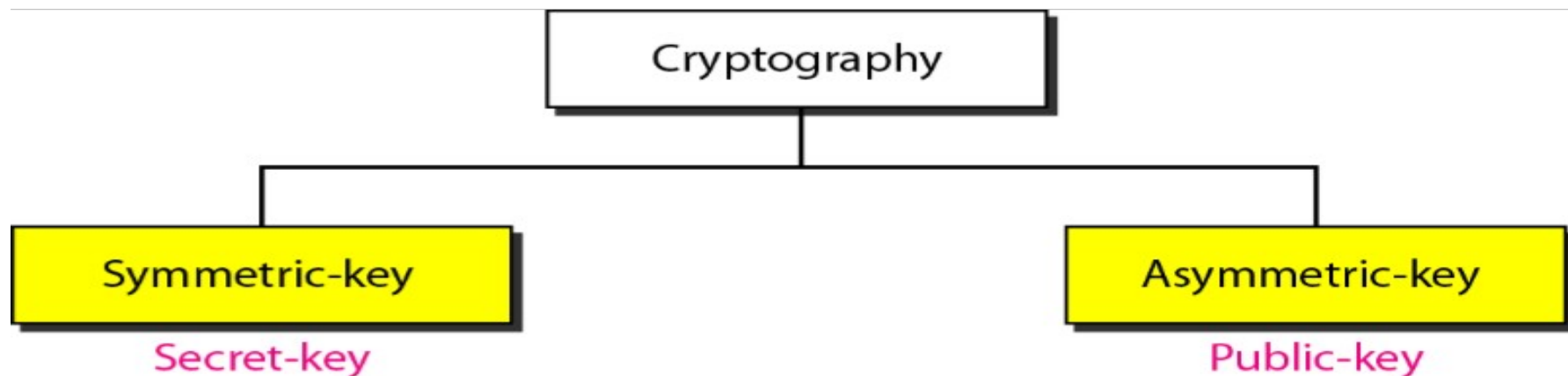
- ❑ The original message, before being transformed, is called **plaintext**. After the message is transformed, it is called **ciphertext**.

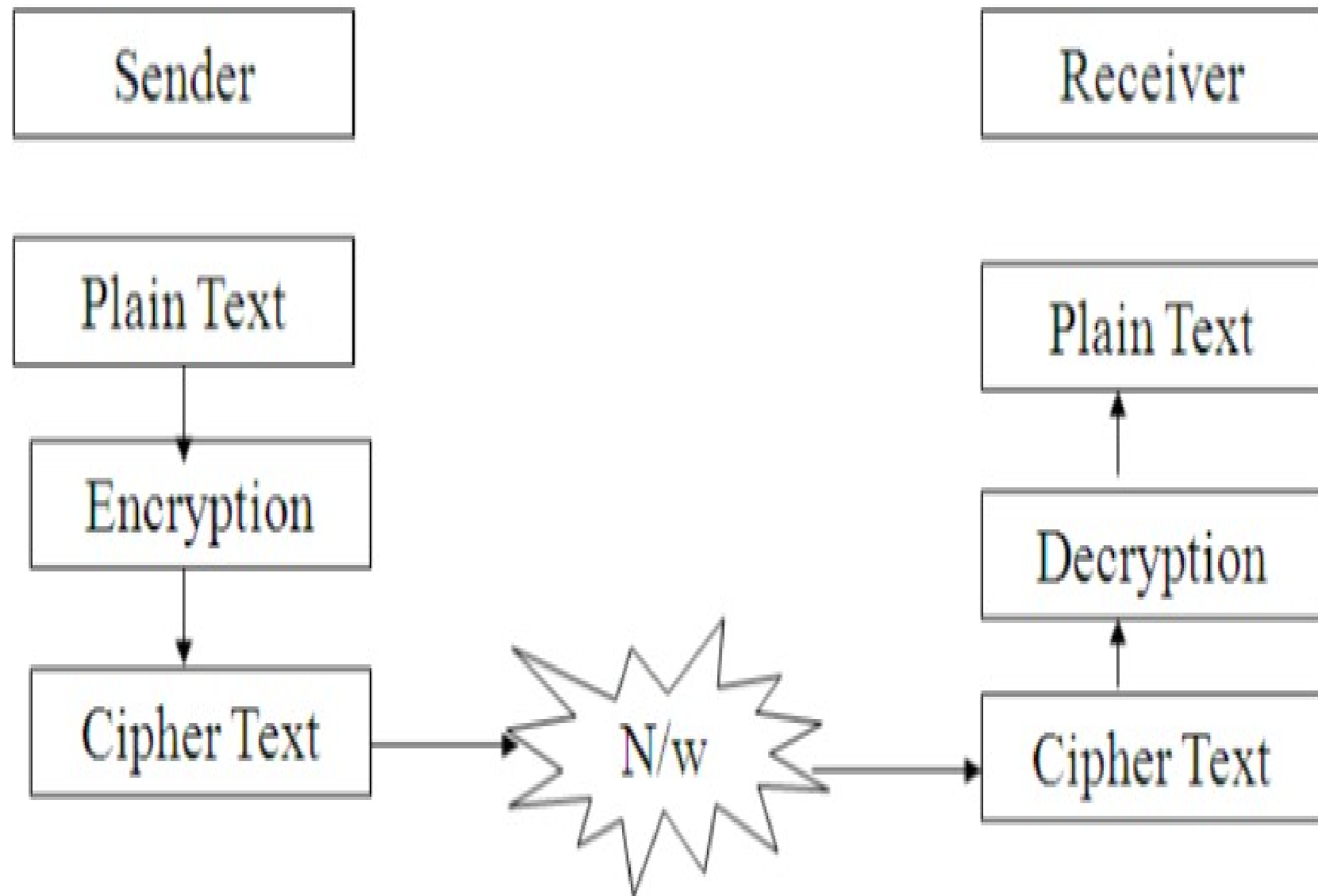


- ❑ The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.



- A **key** is a number (or a set of numbers) that the cipher, as an algorithm, operates on.
- To encrypt a message, we need an **encryption algorithm**, an **encryption key**, and the **plaintext**. These create the ciphertext.
- To decrypt a message, we need a **decryption algorithm**, a **decryption key**, and the **ciphertext**. These reveal the original plaintext.
- We can divide all the cryptography algorithms (ciphers) into two groups: **symmetric-key** (also called **secret-key**) cryptography algorithms and **asymmetric** (also called **public-key**) cryptography algorithms.





Introduction...

- Notation

Given

P=Plaintext

C=CipherText

- $C = E_K (P)$

- $P = D_K (C)$

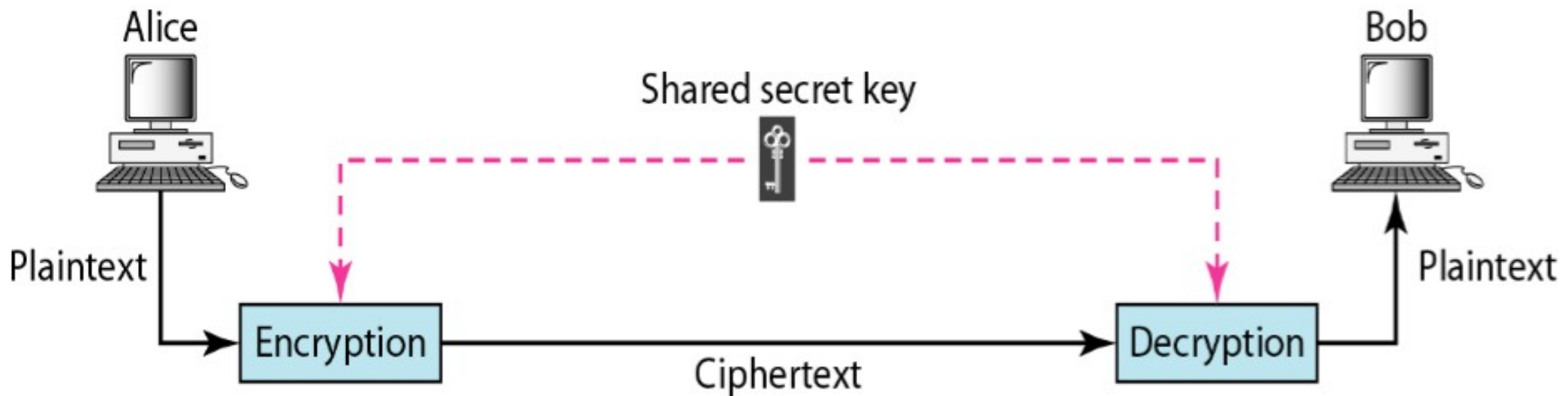
Encryption

Decryption

- Encryption provides :
 - **Confidentiality/Secrecy**
 - keeps our data secret.
 - **Integrity**
 - protect against forgery or tampering

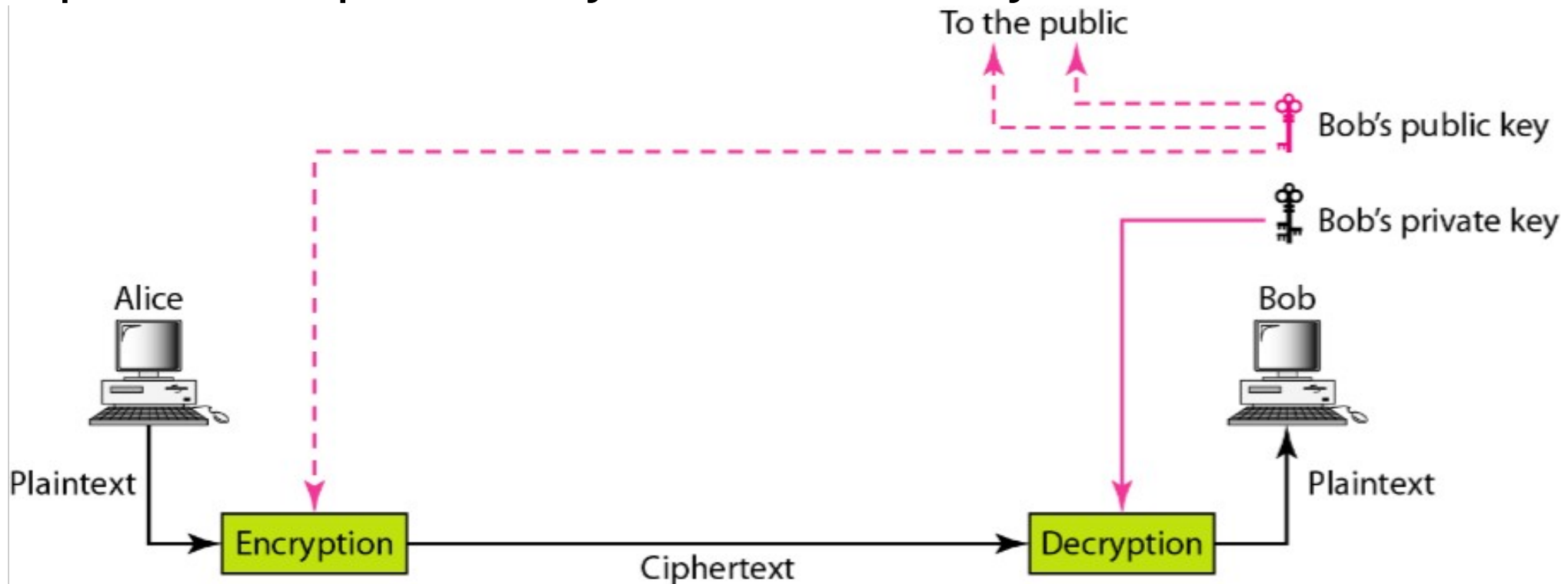
Symmetric-Key Cryptography

- In symmetric-key cryptography, the **same key** is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data



Asymmetric-Key Cryptography

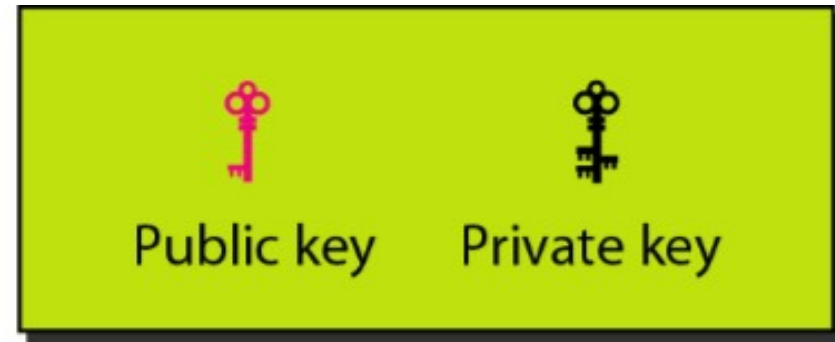
- In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.
- In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual.



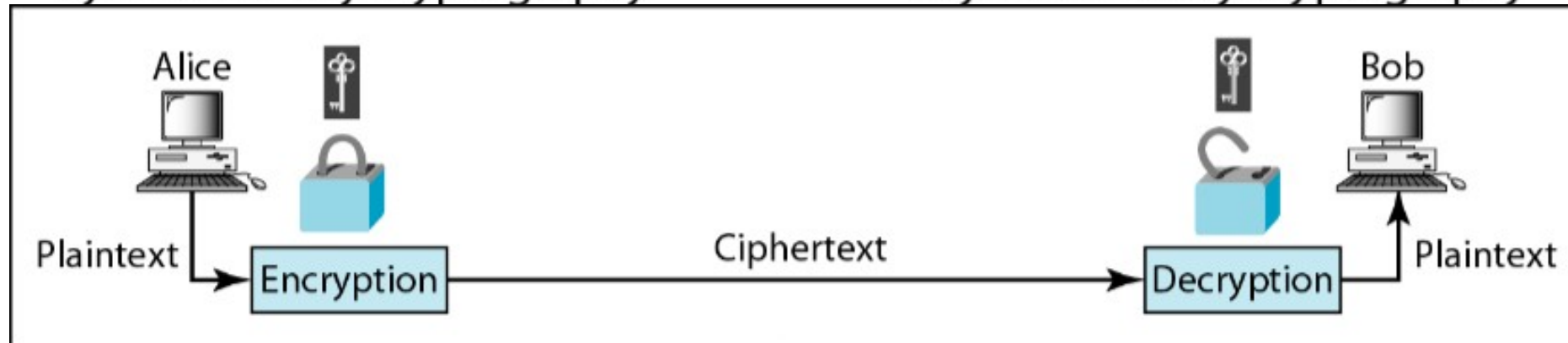
Keys used in cryptography



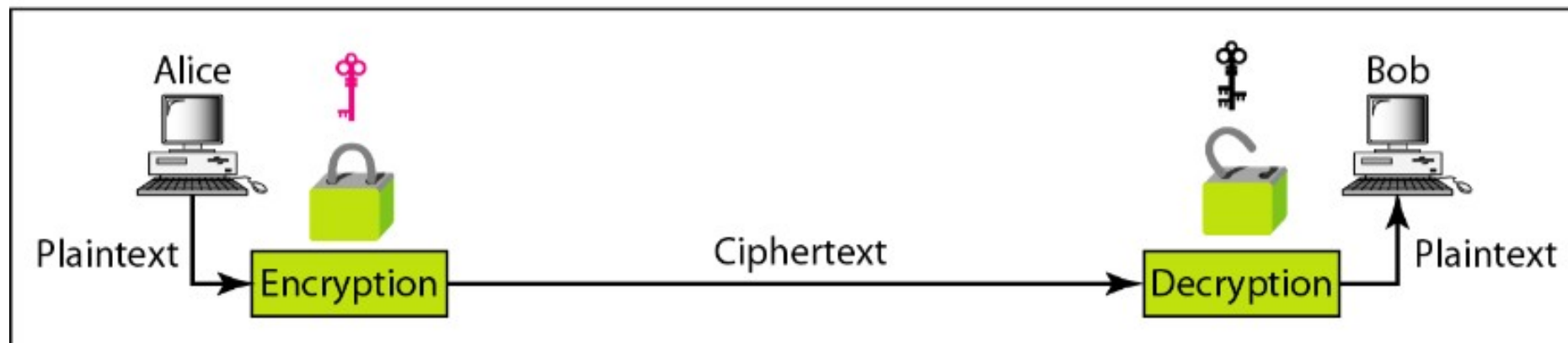
Symmetric-key cryptography



Asymmetric-key cryptography



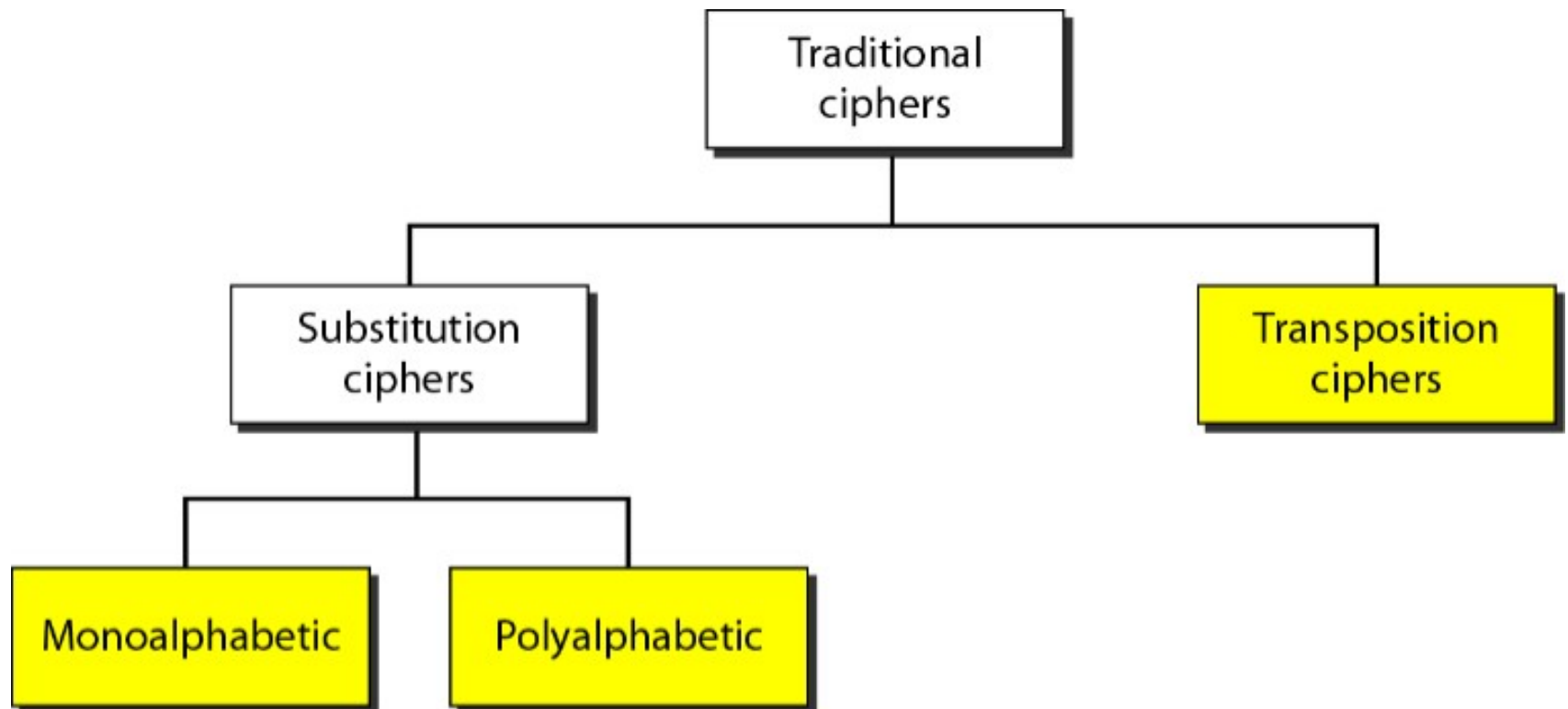
a. Symmetric-key cryptography



b. Asymmetric-key cryptography

SYMMETRIC-KEY CRYPTOGRAPHY

- *Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.*



- ❑ A substitution cipher replaces one symbol with another.
- Example:
The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Solution

The cipher is probably monoalphabetic because both occurrences of L's are encrypted as O's.

Caesar Cipher: used by Julius Caesar's military

- substitutes each letter of the alphabet with the letter standing three places further down the alphabet.

Caesar Cipher

- the algorithm can be expressed as, for each plaintext letter P , substitute ciphertext letter C .

$$\square C = E(3, p) = (p + 3) \bmod 26$$

- mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

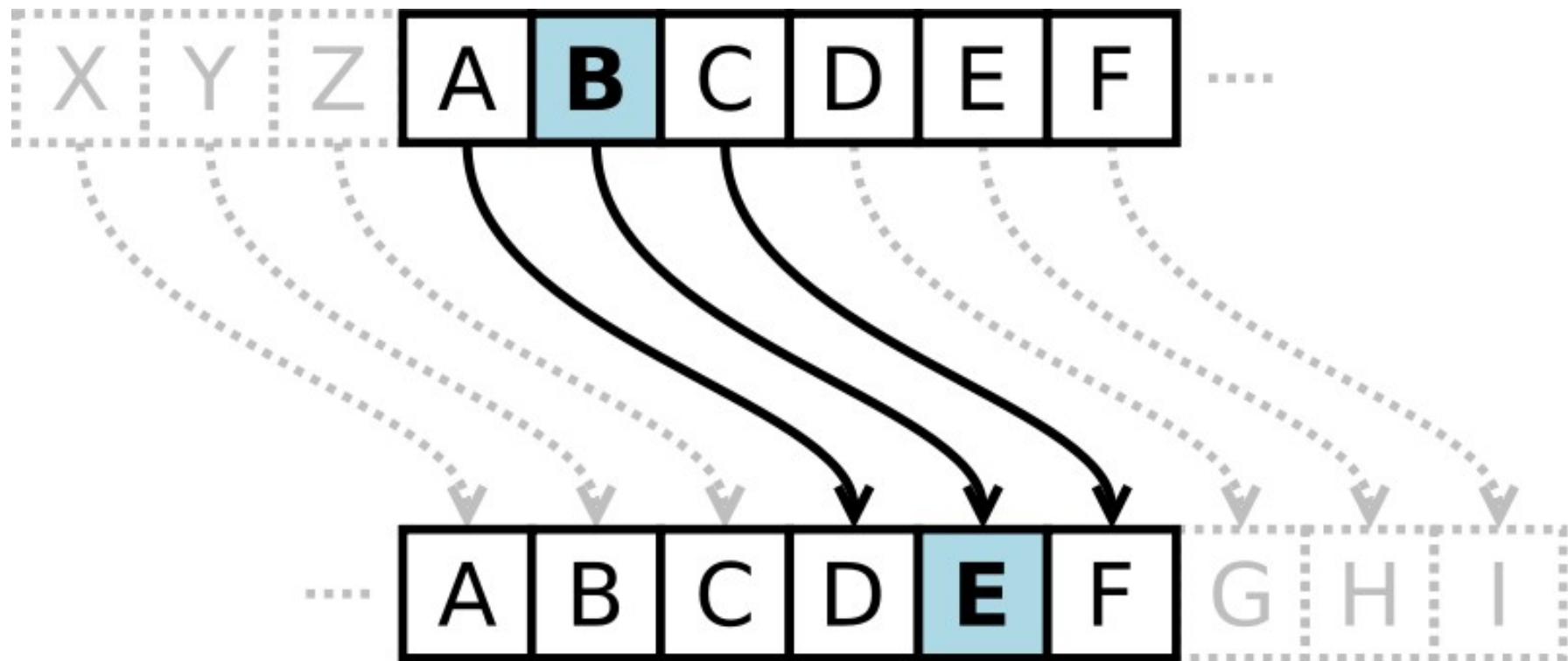
- General Caesar algorithm** as:

$$c = E(k, p) = (p + k) \bmod (26)$$

$$p = D(k, c) = (c - k) \bmod (26)$$

- Where k is [1 to 25]. Secret-key

Caesar cipher



Activity

- Convert it to Caesar Ciphertext?

- Plaintext: are you ready

- Ciphertext: duh brx uhdgb

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

- The shift cipher is sometimes referred to as the Caesar cipher. In this cipher, the encryption algorithm is "shift *key characters down*," with key equal to some number. The decryption algorithm is "shift *key characters up*."
- *Example:*

Use the shift cipher with key = 15 to encrypt the message "HELLO."

Pt:h=07 $E(07+17) \bmod 26$ Ct= 22=w

Solution

*We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is **WTAAD**.*

Example 2

Use the shift cipher with key = 15 to decrypt the message "WTAAD."

Ct:w=22 $D(22-15) \text{MOD} 26$ Pt=07=h

Solution

We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

Playfair Cipher

- Proposed by Charles Wheatstone in 1854
- Named by the name of Wheatstone's friend Lord Playfair
- Used by British army in World War-I, and by Australian in World War-II
 - ✓ Quite fast
 - ✓ Used to protect important, but not very critical information

Creation and Population of Matrix

- ✓ Uses matrix of 5 X 5
- ✓ Used to store the keyword
- ✓ Enter the keyword in the matrix row-wise
- ✓ Drop duplicate letters
- ✓ Fill the remaining spaces with the rest of the English alphabets
- ✓ Both I and J has same precedence

Keyword: NETWORK SECURITY

N	E	T	W	O
R	K	S	C	U
I	Y	A	B	D
F	G	H	L	M
P	Q	V	X	Z

Encryption Process

- ✓ The PT message is broken down into groups of 2 alphabets
- ✓ If both alphabets are same or only one is left, add X after the alphabet
- ✓ If one character is ' ', then that character will be replaced by the respective character in the previous pair
- ✓ If both the alphabets in the pair is in the same row of the matrix, replace them with alphabets to their immediate right respectively. If the original pair is on the right side of the row , then wrapping around to the left side of the same row happens
- ✓ If both the alphabets in the pair appears in the same column of the matrix, replace them with alphabets immediately below them respectively . If the original pair is on the bottom side of the column, then wrapping round to the top side of the same column happens
- ✓ If the alphabets are not in the same row or column, replace them with the alphabets in the same row respectively, but at the other pair of corners of the rectangle defined by the original pair. The 1st encrypted alphabet of the pair is the one that is present on the same row as the 1st PT alphabet

CONT....

Keyword: NETWORK SECURITY

PT: HAPPY NEW YEAR

HA PP YN EW YE AR → HA PX YN EW YE AR

HA	PX	YN	EW	YE	AR
VH	QZ	IE	TO	GK	IS

CT:VHQZIETOGKIS

To decrypt the message, simply reverse the entire process. Break the CT into pairs of letters

IPSec Security Features

- ❑ IPSec is the most secure method commercially available for connecting network sites.
- ❑ IPSec was designed to provide the following security features when transferring packets across networks:
 - ✓ **Authentication:** Verifies that the packet received is actually from the claimed sender.
 - ✓ **Integrity:** Ensures that the contents of the packet did not change in transit.
 - ✓ **Confidentiality:** Conceals the message content through encryption.

IPSec contains the following elements:

- ✓ **Encapsulating Security Payload (ESP):** Provides confidentiality, authentication, and integrity.
- ✓ **Authentication Header (AH):** Provides authentication and integrity.
- ✓ **Internet Key Exchange (IKE):** Provides key management and Security Association (SA) management.

Security Policy Design Issues

What is the company's desired level of security?

How much money is the company willing to invest in security?

If the company is serious about restricting access through an Internet link, what about restricting access through all other entry ways?

The company must have a well-designed security policy.

10 Tips for Computer Network Security

1. Use a good anti-virus program.
2. Make sure your virus definitions are up-to-date.
3. Run regular virus scans.
4. Update your operating system regularly.
5. Configure and use a firewall.
6. Use your Web browser's security features.
7. Enable your router's security features.
8. Install an anti-spyware program.
9. Use strong, varied passwords.
10. Consider a computer network security suite and policy. .

Quiz 5%

1. Decrypt the CT:VHQZIEТОGKIS using playfair cipher.