Chapter -7

SECURITY AND PROTECTION

What is security?

- **Security** usually refers to ensuring that:
  - Users can perform only the tasks that they are authorized to do; and
  - Can obtain only the information that they are authorized to have.

- **Why Security?**
  - Security relates to a “security objective” or “security policy.
  - **Why is this important?**

    1. To prevent theft of or damage to the hardware,
    2. To prevent theft of or damage to the information, and
    3. To prevent disruption or interruption of service .

Cont.…

- Security must occur at **four levels** to be effective:
- ***Physical***
  - Data centers, servers, connected terminals.
- ***Human***
  - Avoid social engineering, phishing, and dumpster diving.
- ***Operating System***
  - Protection mechanisms, debugging.
- ***Network***
  - Intercepted communications, interruption, DOS.

Computer security

- Protecting a single computer with one user is easy.
  - Prevent everybody else from having access.
  - Encrypt all data with a key only one person knows.
- Sharing resources safely is hard.
  - Preventing some people from reading private data (**e.g. grades**).
  - Prevent some people from using too many resources (**e.g. disk space**).
  - Prevent some people from interfering with other programs (**e.g. inserting keystrokes/modifying displays**).

Why is security hard?

- Security **slows** things down.
- Security **gets** in the way.
- Security **adds no value** if there are no attacks.
- Only the government used to pay for security.
- The Internet made us all potential victims.

Computer protection and security mechanisms

- Provided by an operating system must address the following requirements: **Confidentiality, Integrity, Availability**, and **Authenticity**.

- ***Confidentiality*:-** (or ***privacy***) the requirement that information maintained by a computer system be accessible only by **authorized parties** (users and the processes that run as/represent those users).

- ***Integrity***:- the requirement that a computer system's resources can be modified **only by authorized parties.**
  - *Modification* occurs when an unauthorized party not only gains access to but changes a resource such as data or the execution of a running process.

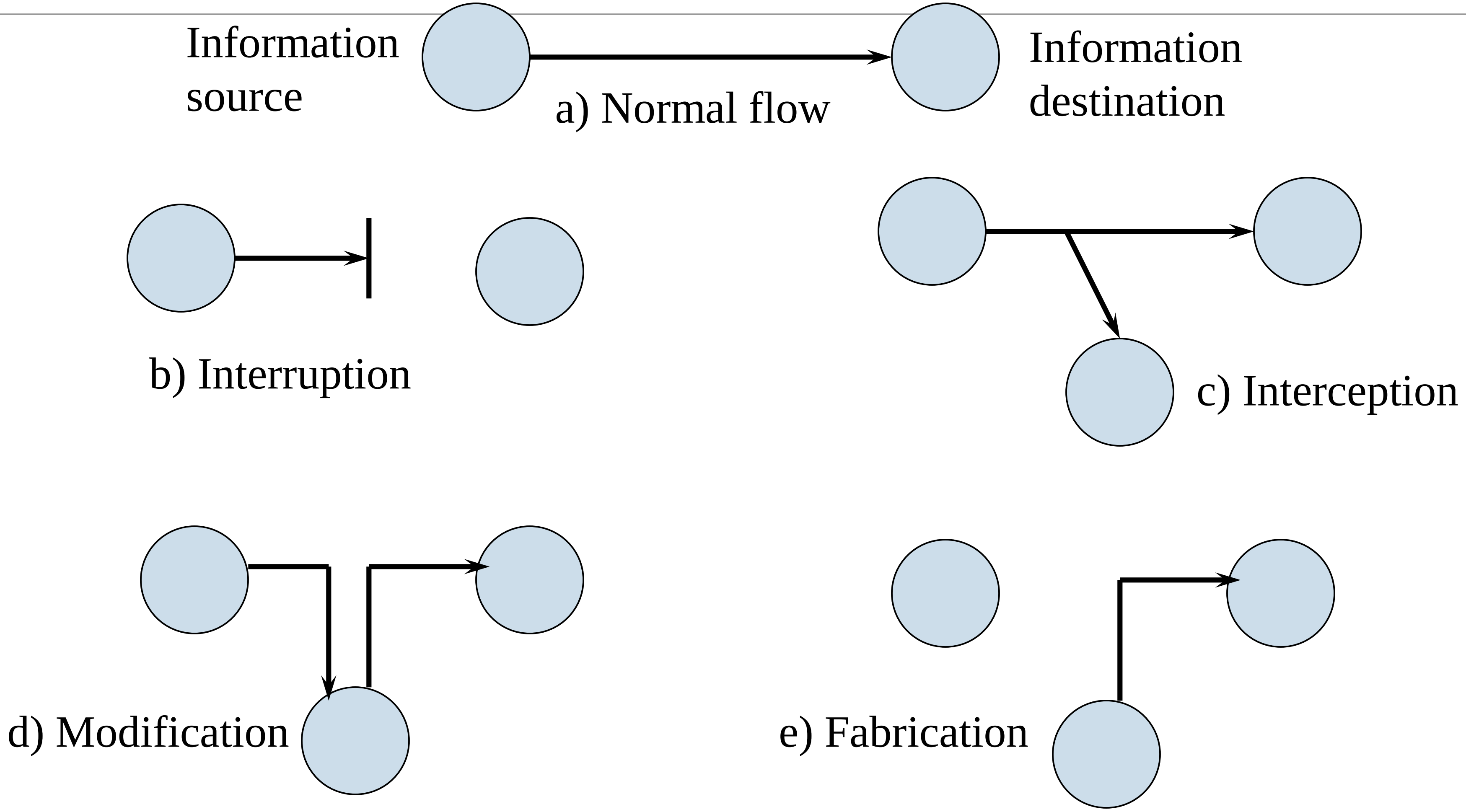
Cont..

- ***Availability*:-** the requirement that a computer system be accessible at required times by authorized parties.

- **Security threats:**
  - ***Interruption*** occurs when an unauthorized party reduces the availability of or to a resource.

- ***Authenticity* is** the requirement that a computer system can verify the identity of a user.
  - ***Fabrication* occurs** when an unauthorized party inserts counterfeit data amongst valid data.
  - The main types of **authentication** needed in the **operating system** are **passwords.**

Cont………….(Security threats)



Cont.…

- ***Password*** correct identification at the time of login is crucial to the functioning of a secure system.
  - Because all access control decisions and accounting functions are based on this identity.
- To **provide good security**, a password-based authentication system must have mechanisms for the following:
  - Keep password secret
  - Making passwords difficult to guess
  - Limiting damages done by a compromised password
  - Identifying and discouraging unauthorized user logins.

Password Vulnerability

- Passwords are extremely common.
- Passwords can often be guessed.
- Use of mechanisms to keep passwords secret does not guarantee that the system security cannot be broken.
- Some techniques that may be used to make the task of guessing a password difficult are as follows:
  - Longer passwords
  - Salting the password table
  - System assistance in password selection

Assets and their Vulnerabilities

- **Hardware** is mainly vulnerable to interruption, either by theft or by Vandalism.
- **Physical security measures** are used to prevent these attacks.
- **Software** is also vulnerable to interruption, as it is very easy to delete.
- **Backups** are used to limit the damage caused by deletion.
- **Modification** or **fabrication** through alteration (e.g. by viruses) is a major problem, as it can be hard to spot quickly.
- **Software** is also vulnerable to interception through unauthorized copying: this problem is still largely unsolved.

Cont..

- **Data is vulnerable in many ways:**

- **Interruption** can occur through the simple destruction of data files.

- **Interception** can occur through unauthorized reading of data files, or more perniciously through unauthorized analysis and aggregation of data.

- **Modification and fabrication** are also obvious problems with potentially huge consequences.

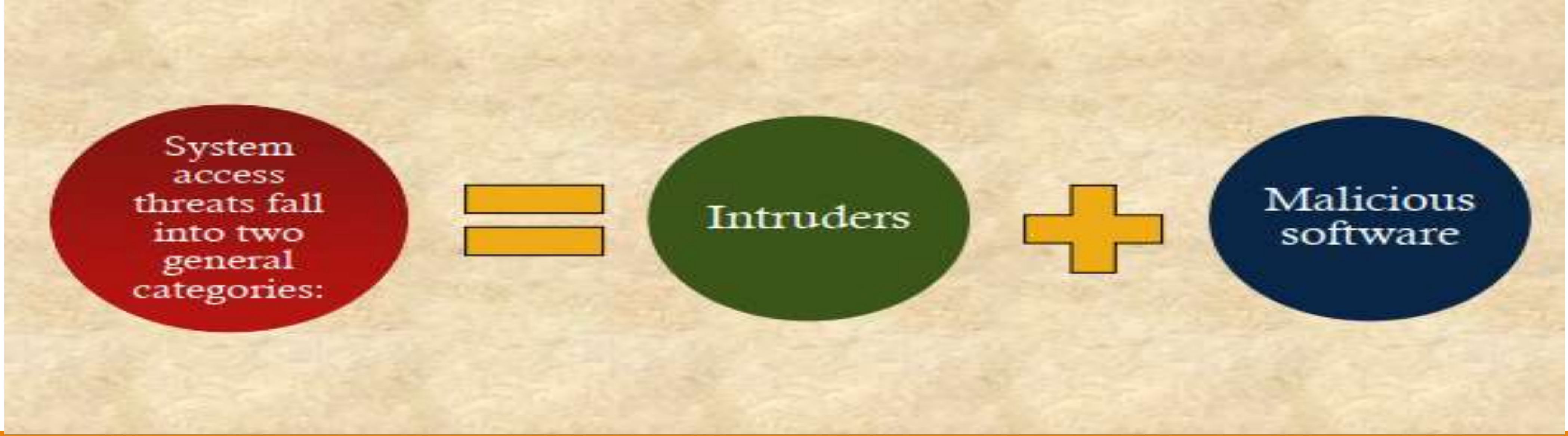
- **Communications** are vulnerable to all types of threats.

- ***Passive attacks*** take the form of eavesdropping and fall into two categories:
  - Reading the contents of a message, or more subtly,
  - Analyzing patterns of traffic to infer the nature of even secure messages.

- Passive attacks are hard to detect, so the importance is usually on prevention.

Cont..

- *Active attacks* involve the modification of a data stream or the creation of a false data stream.
  - One entity may *masquerade* as another (presumably one with more or different privileges), maybe by capturing and replaying a verification sequence.



Intruders

- **Intruders** and **viruses** are the two most publicized security threats.

Three classes of intruders:

- **A masquerader** is an unauthorized individual (**an outsider**) who penetrates a system to exploit legitimate users’ accounts.
- **A misfeasor** is a legitimate user (**an insider**) who accesses resources to which they are not privileged, or who abuses such privilege.
- **A clandestine user** is an individual (**an insider or an outsider**) who seizes control of a system to evade auditing controls, or to suppress audit collection.

Cont..

- **Intruders** are usually trying to gain access to a system or to increase privileges to which they are not entitled, often by obtaining the password for a **legitimate account.**
- **Many methods of obtaining passwords have been tried:**
  - Trying default passwords.
  - Exhaustively testing short passwords.
  - Trying words from a dictionary, or a list of common passwords.
  - Collecting personal information about users.
  - Using a Trojan horse.
  - Eavesdropping on communication lines.
- The **usual methods** for protecting passwords are through one-way encryption, or by limiting access to password files. However, passwords are inherently vulnerable.

Malicious Software

- The most sophisticated threats to computer systems are through malicious software, sometimes called ***malware***.
- **The malware** attempts to cause damage to or consume the resources of a target system.
- Programs that exploit vulnerabilities in computing systems are also referred to as **malware**.
- Can be divided into **two categories** **Parasitic** and **independent**:
  - ***Parasitic malware:*** fragments of programs that cannot exist independently of some **actual application program, utility, or system programs.** viruses, logic bombs, and backdoors are examples.

Cont..

- ***Independent malware:*** Self-contained programs that can be scheduled and run by the operating system. Worms and bot programs are examples.
  - Malware can be divided into programs that can operate independently, those that need a host program; and also into programs that can replicate themselves, and those that cannot.

- **A trap door**: is a secret entry point into a program, often left by the **program's, developers**, or sometimes delivered via a software update.

- **A logic bomb:** Is code embedded in a program that ”explodes” when certain conditions are met. **e.g.** a certain date or the presence of certain files or users.

- Logic bombs also often originate with the developers of the software.

Cont..

- **A Trojan horse** is a program that contains hidden code to perform some unwanted or harmful function.
- **A virus** is a program that can ”infect” other programs by modification, as well as causing local damage.
  - Such modification includes a copy of the virus, which can then spread further to other programs.
- **Zombie** is an independent program that secretly takes over a system and uses that system to launch attacks on other systems. Such attacks often involve further replication of the zombie itself.
- Zombies are often used in denial-of-service attacks. The last three of these involve replication.
- In all cases, prevention is **much** easier than detection and recovery.

Cryptography as a Security
From ancient Ciphers to Modern Cryptosystems

- **Cryptography**
  - Secures information by encrypting it.
  - **Cryptography** – the study of encryption principles/methods.

- **Plaintext** - original message.
- **Cipher text -** coded message.
- **Cipher -** algorithm for transforming plaintext to cipher text.
- **Key -** info used in cipher known only to sender/receiver.
- **Encipher (encrypt)** - converting plaintext to cipher text.
- **Decipher (decrypt)** - converting cipher text to plaintext.
- **Cryptanalysis (code breaking)** – the study of principles/ methods of deciphering cipher text *without* knowing the key.
- **Cryptology -** field of both cryptography and cryptanalysis.

Cryptography as a Security

- With a given computer the transmittal of messages is safe, reliable, and secure.
  - Because OS knows exactly where each one is coming from and where it is going on a network, however, things aren't so straightforward.
- ***For example*** in e-mail sender may spoof their identity, and outgoing packets are delivered to a lot of other computers.
- Besides, the final destination brings up two big questions about security.
- **Trust -** How can the system be sure that the messages received are really from the source that they say they are, and can that source be trusted?

Cont.…

- **Confidentiality -** How can one ensure that the messages one is sending are received only by the intended recipient? Cryptography can help with both of these problems, through a system of **secrets** and **keys.**
- In the former case, the **key is held by the sender** so, that the recipient knows that only the authentic author could have sent the message.
- In the latter, the **key is held by the recipient**, so that only the intended recipient can receive the message accurately.

Encryption

- It is the conversion of plaintext to cipher text.
- The basic idea of encryption is to encode a message so that only the favorite recipient can decode and read it.
- Encryption has been around since before the days of Caesar and is an entire field of study in itself.

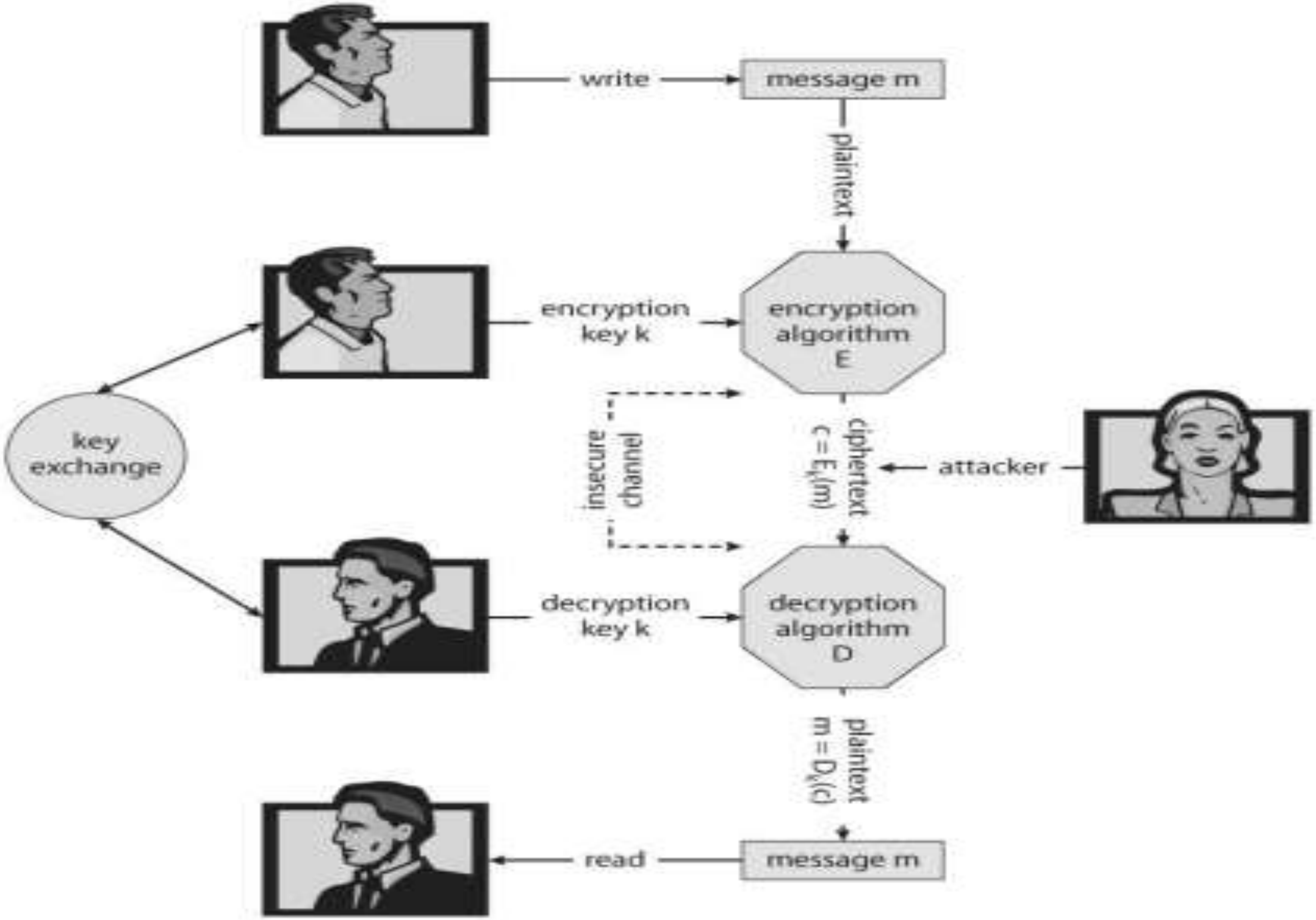
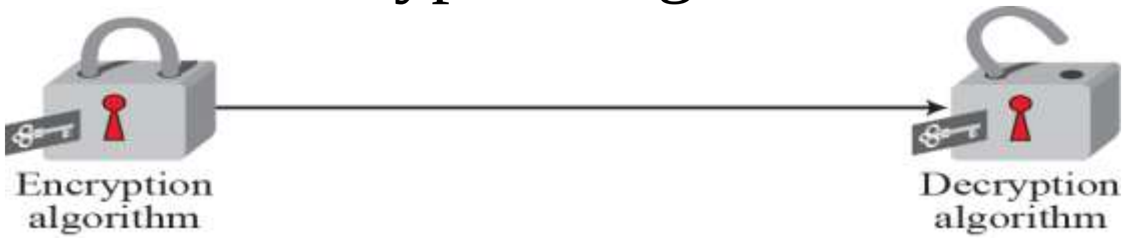


Figure - A secure communication over an insecure medium.

Types of encryptions

❑**Symmetric Encryption:** With ***symmetric encryption*** the same key is used for both encryption and decryption and must be safely guarded.

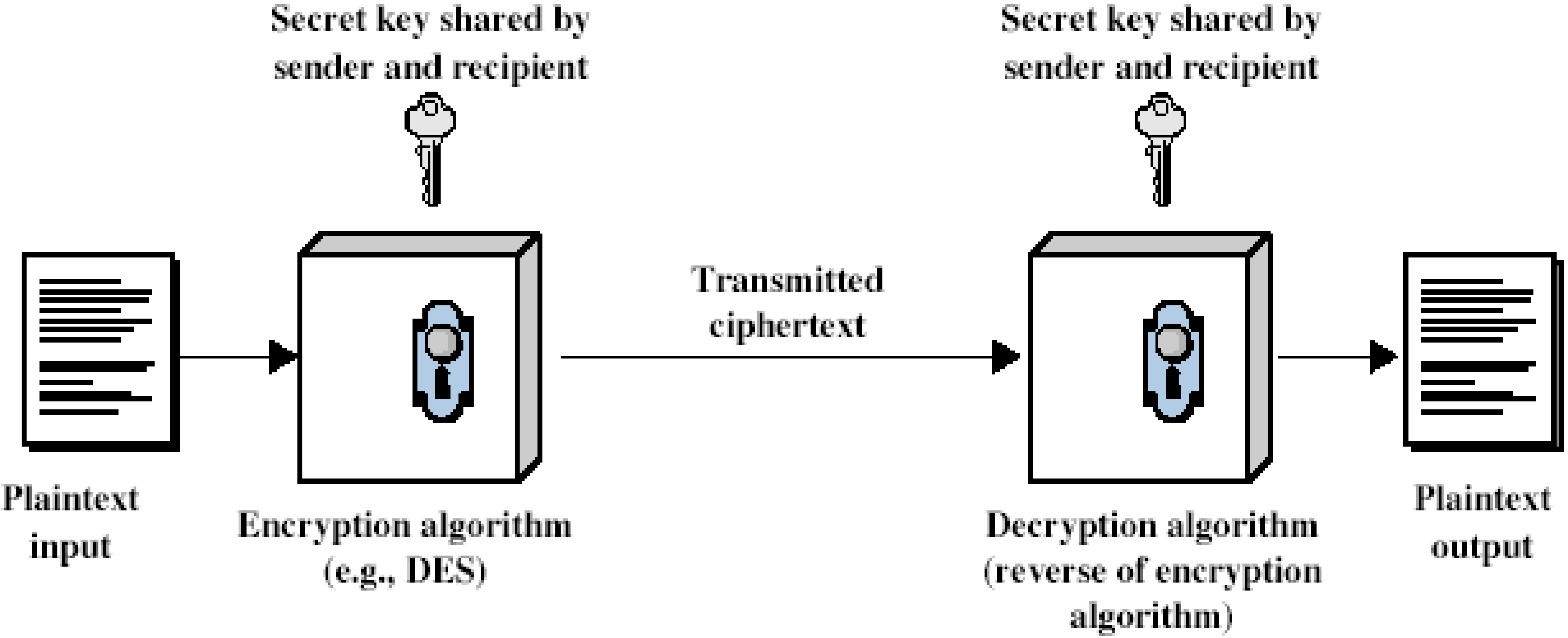
➢There are a number of well-known symmetric encryption algorithms that have been used for computer security.



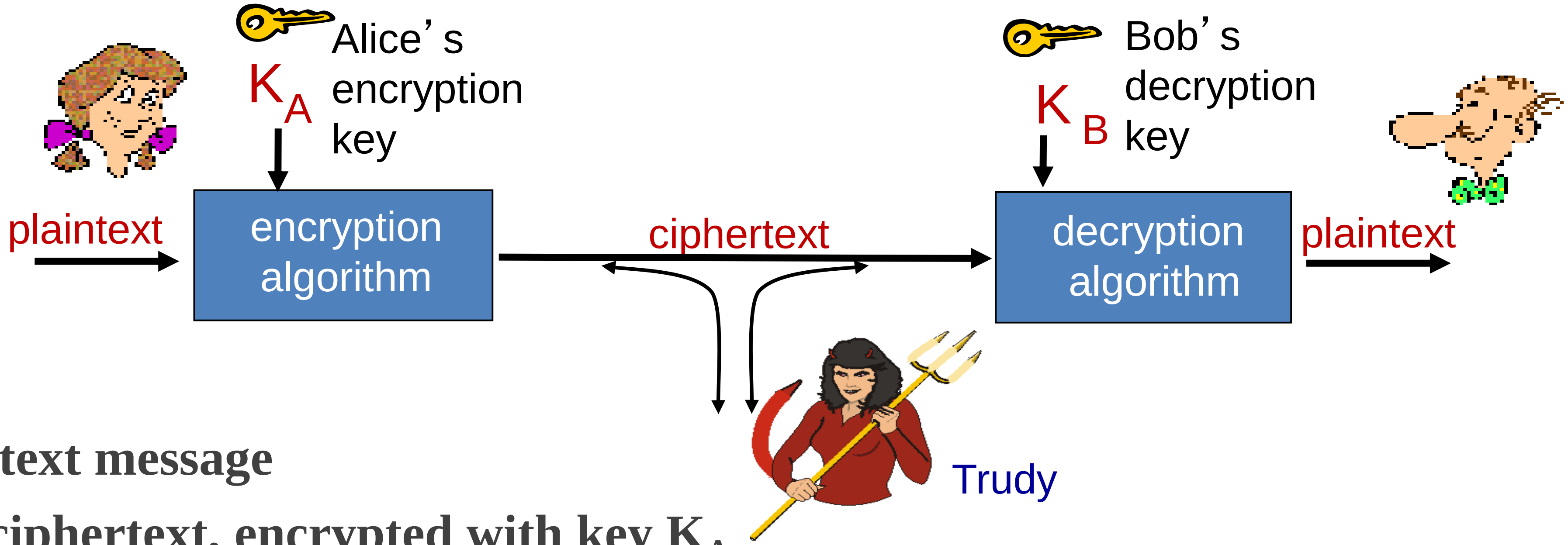
❑ ***Asymmetric encryption:*** The decryption key is not the same as the encryption key, and more importantly cannot be derived from it.

➢Which means the encryption key can be made publicly available, and only the decryption key needs to be kept secret. (or vice-versa, depending on the application).

Symmetric Cipher Model


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Symmetric Key Cryptography



m plaintext message

K_A(m) ciphertext, encrypted with key K_A

m = K_B(K_A(m))

- symmetric key crypto: **Bob** and **Alice** share know same (symmetric) key: **K**

How to prevent OS from Attack ?

- Performing regular OS patch updates.
- Installing updated antivirus engines and software.
- Examining all incoming and outgoing network traffic through a firewall.
- Creating secure accounts with required privileges only (i.e., user management).

Firewalls

- The firewall acts as a choke point so that all incoming traffic and all outgoing traffic must pass through the firewall.
- The firewall enforces the local security policy, which defines the traffic that is authorized to pass.
- The firewall is secure against attacks.

Antivirus

- **Antivirus** software helps protect your computer against malware and cybercriminals.
- **Antivirus** software looks at data web pages, files, software, and applications traveling over the network to your devices.
- It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior.

End of Chapter Seven

Question ?