جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذة المادة:

م. سماح فخري عزيز

Encryption

CONTENTS

- **Basic classification of encryption**
- **Symmetric-key or (or secret-key)**
- **Asymmetric (or public-key)**
- **The key**
- **The General Requirements of Cryptosystem**
- **Components of a Cryptosystem**
- **Basic Cryptographic Algorithms**

BASIC CLASSIFICATION OF ENCRYPTION KEY-BASED ALGORITHMS

❑Symmetric-key or (or secret-key)

❑Asymmetric (or public-key)

Symmetric-key or (or secret-key)

- ***Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key)***

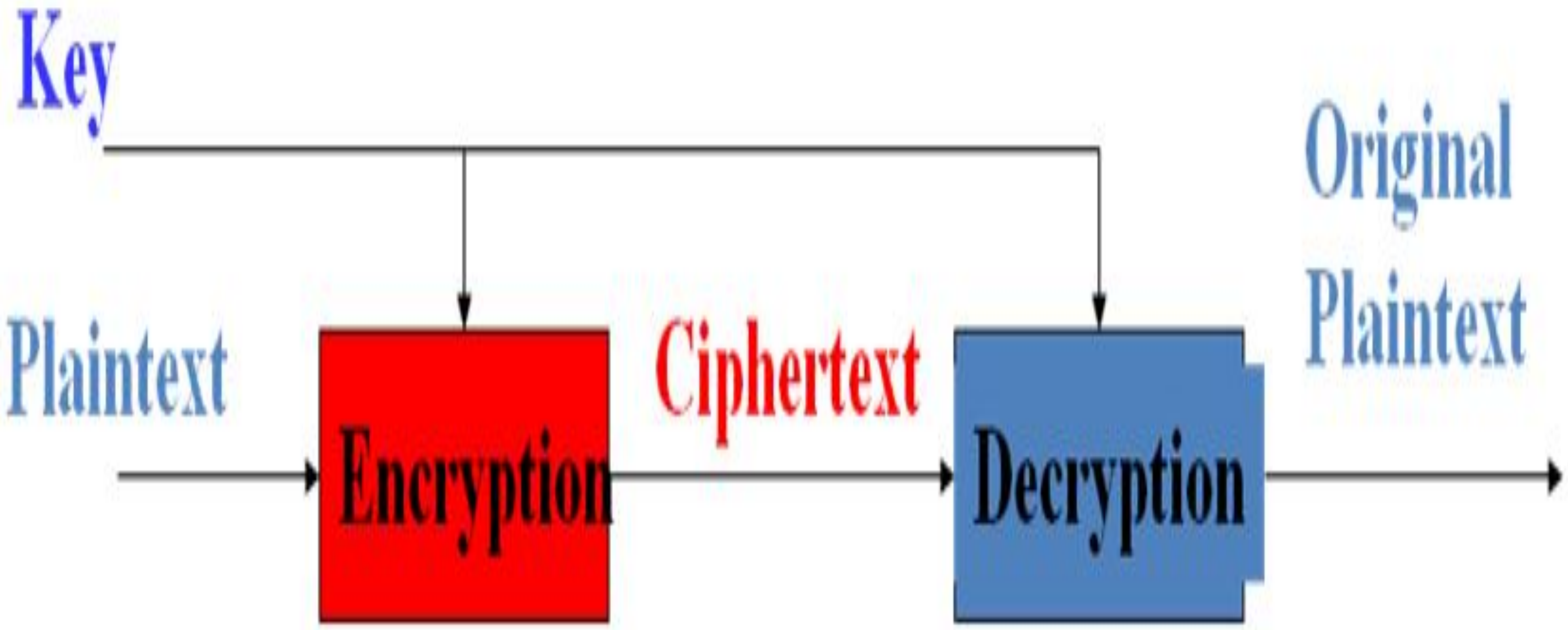
SYMMETRIC-KEY OR (OR SECRET-KEY)

- **two main types:**

- **stream ciphers** – operate on individual characters of the plaintext

- **block ciphers** – process the plaintext in larger blocks of characters

Symmetric Encryption



Asymmetric (or public-key)

- algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

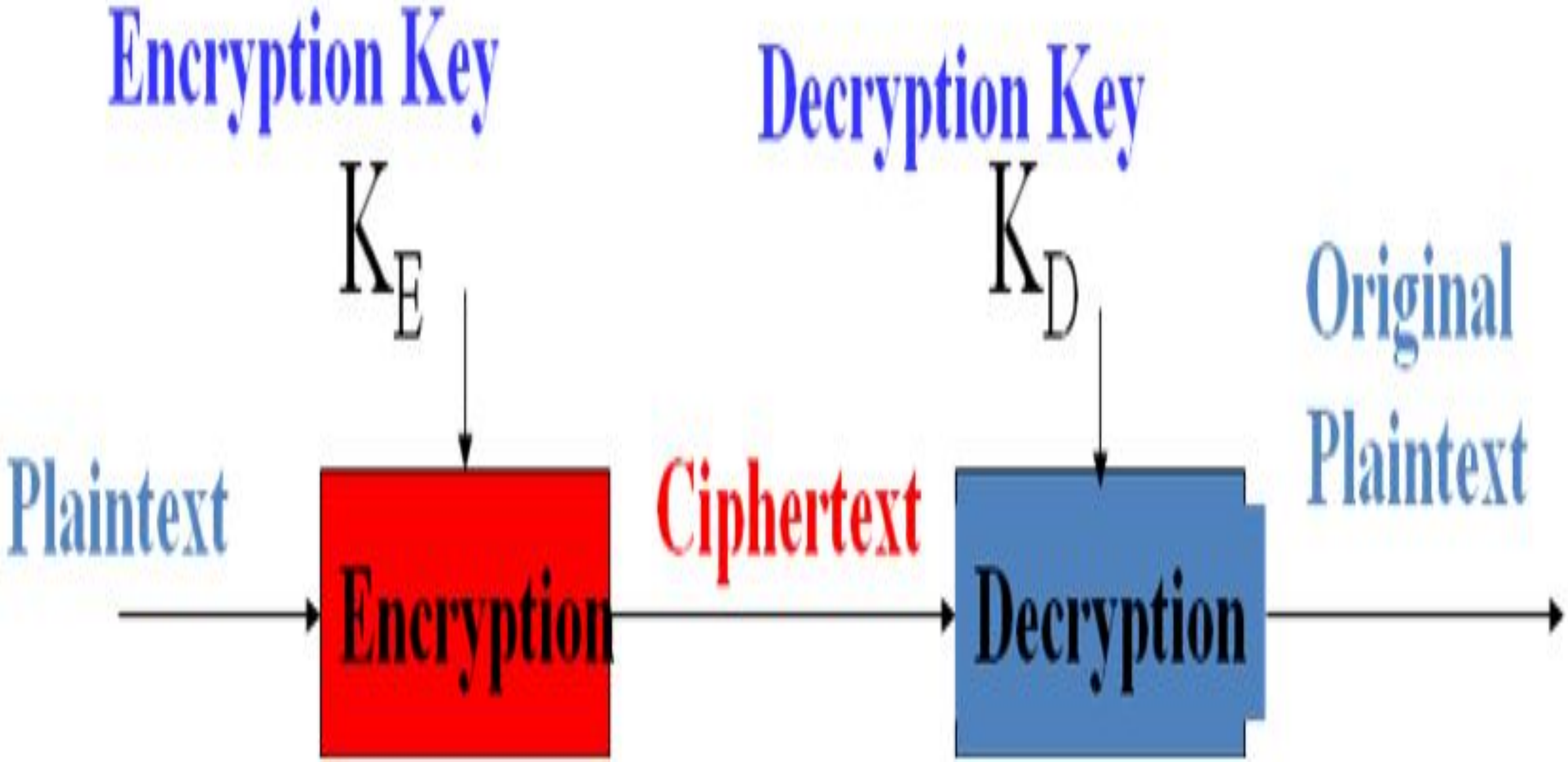
- permit the encryption key to be public, allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message.

THE KEY

- ***The encryption key is also called the public key***

- ***The decryption key the private key or secret key.***

Asymmetric Encryption



THE GENERAL REQUIREMENTS OF CRYPTOSYSTEM

- ***Cryptosystem must satisfy three general requirements:***
- **1) The enciphering and deciphering transformations must be efficient for all keys.**
- **2) The system must be easy to use.**
- **3) The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms Encryption or Decryption.**

COMPONENTS OF A CRYPTOSYSTEM

- **The various components of a basic cryptosystem are as follows : -**

- **Plaintext.** It is the data to be protected during transmission.

ENCRYPTION ALGORITHM

- It *is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.*

CIPHERTEXT

- *It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.*

DECRYPTION ALGORITHM

- *It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.*

ENCRYPTION KEY & DECRYPTION KEY

- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

ENCRYPTION KEY & DECRYPTION KEY

- **Decryption Key** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

KEY SPACE

- For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

BASIC CRYPTOGRAPHIC ALGORITHMS

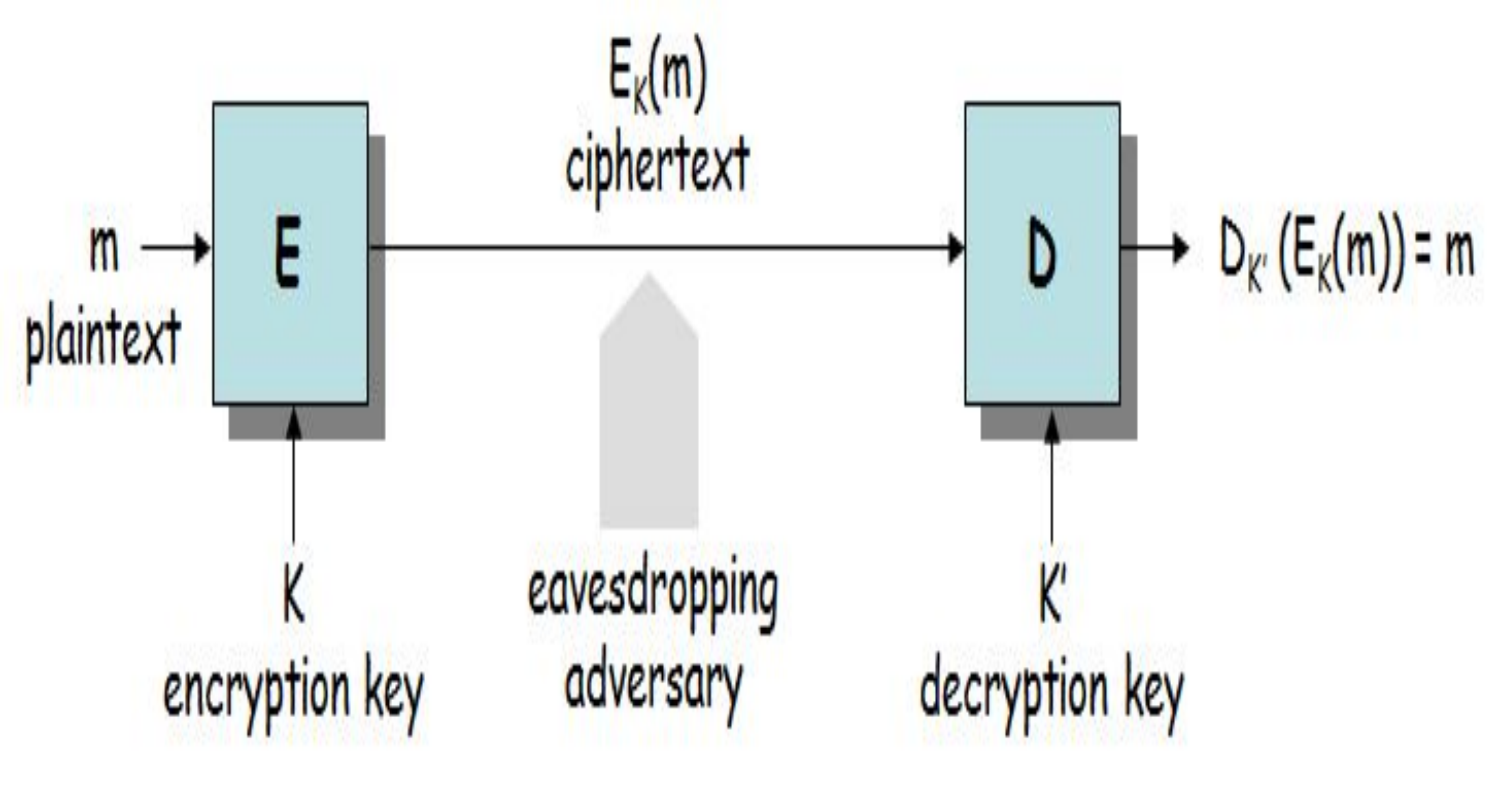
- A **cipher** is the method of encryption and decryption.

- Some cryptographic methods rely on the secrecy of the algorithms.
- **Keyless Cipher** is a cipher that does not require the use of a key.

BASIC CRYPTOGRAPHIC ALGORITHMS

- All modern algorithms use a **key** to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.
- The key used for decryption can be different from the encryption key, but for most algorithms they are the same.

CLASSICAL MODEL OF ENCRYPTION



Thank you