



كلية الرشيد الجامعة قسم هندسة تقنيات الحاسوب

المرحلة الرابعة

أمنية الحاسوب و شبكاتها

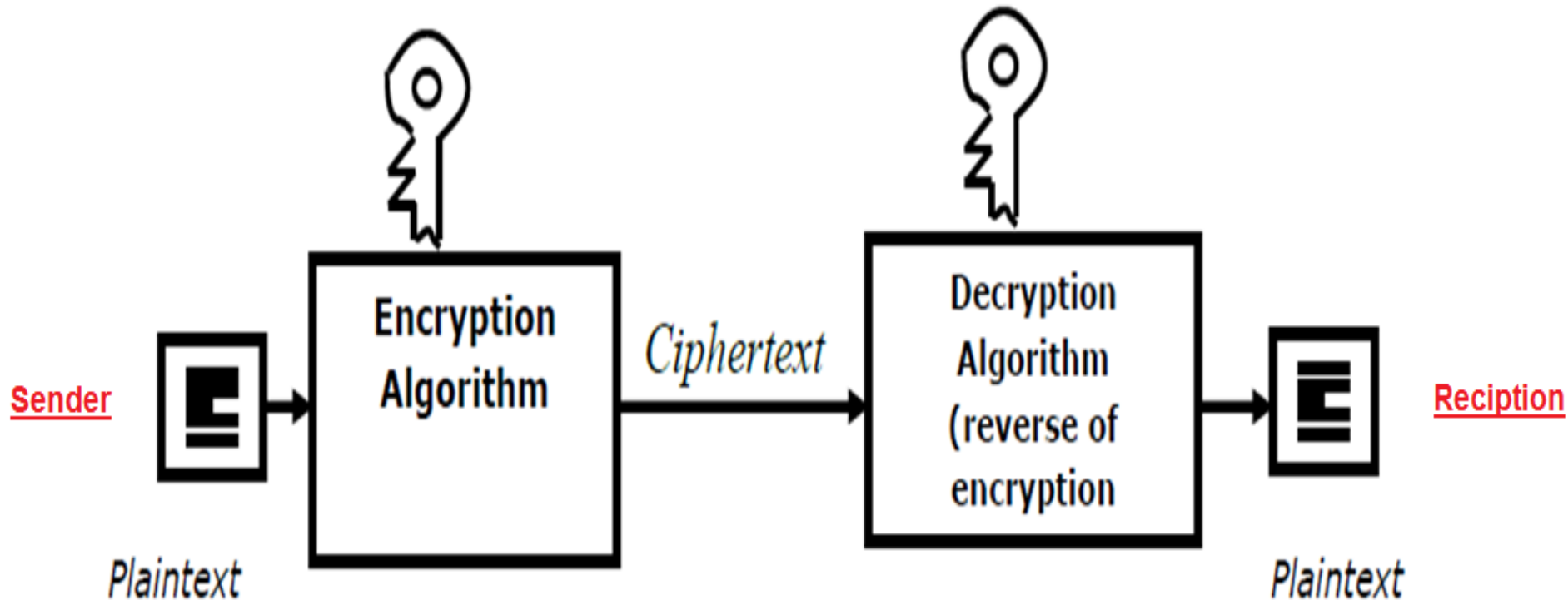
المحاضرة رقم (٢)

مدرس المادة : م.م. تميم محمد

CRYPTOGRAPHY

Secret key shared by sender & recipient

Secret key shared by sender & recipient



Simplified Model of Conventional Encryption

CRYPTOGRAPHY

- ❑ **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- ❑ **Ciphertext:** is the unintelligible message, produced as output. It depends on the plaintext and the secret key.
- ❑ **Secret key:**
 - The secret key is a secret information used as input to the algorithm.
 - The key is a value independent of the plaintext and the algorithm.
 - The algorithm will produce a different output depending on the specific key being used at the time.
 - The exact substitutions and transformations performed by the algorithm depend on the key.

CRYPTOGRAPHY

❖ Encryption Algorithm:

- Is the process of transforming plaintext into ciphertext.
- It takes the original plaintext and the secret key to produces the ciphertext.

❖ Decryption Algorithm:

- Is the process of transforming ciphertext into plaintext.
- It takes the ciphertext and the secret key to produces the original plaintext.

NOTE:

Encryption Process

Plaintext → small letter

Key → capital letter

Cipher text → capital letter

Decryption Process

Cipher text → capital letter

Key → small letter

Plain text → small letter

CLASSIFICATION OF CRYPTOGRAPHY

1. Number of keys used

- Hash functions: no key
- Symmetric encryption (Private Key): one key
- Asymmetric encryption (Public Key): two keys - public, private

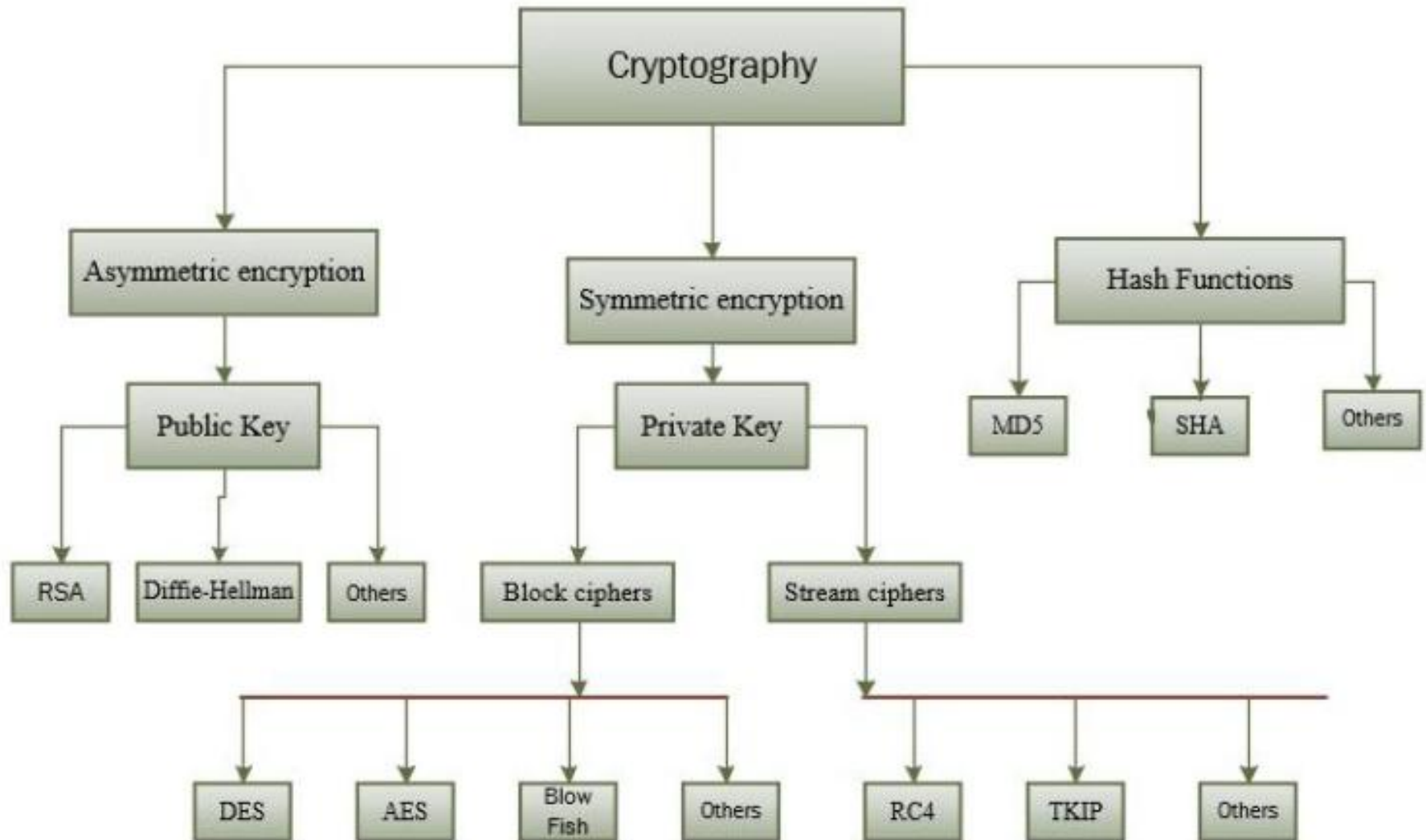
2. Type of encryption operations used

- substitution / transposition / product

3. Way in which plaintext is processed

- block / stream

CLASSIFICATION OF CRYPTOGRAPHY



❖ **Block Cipher:**

processes the input one block of elements at a time, producing an output block for each input block.

❖ **Stream Cipher:**

processes that encrypt a digital data stream one bit or one byte at a time.

❖ **Monoalphabetic:**

Using one alphabet - refers to a cryptosystem where each alphabetic character is mapped to a unique alphabetic character

❖ **Polyalphabetic:**

Using many alphabets - refers to a cipher where each alphabetic character can be mapped to one of many possible alphabetic characters