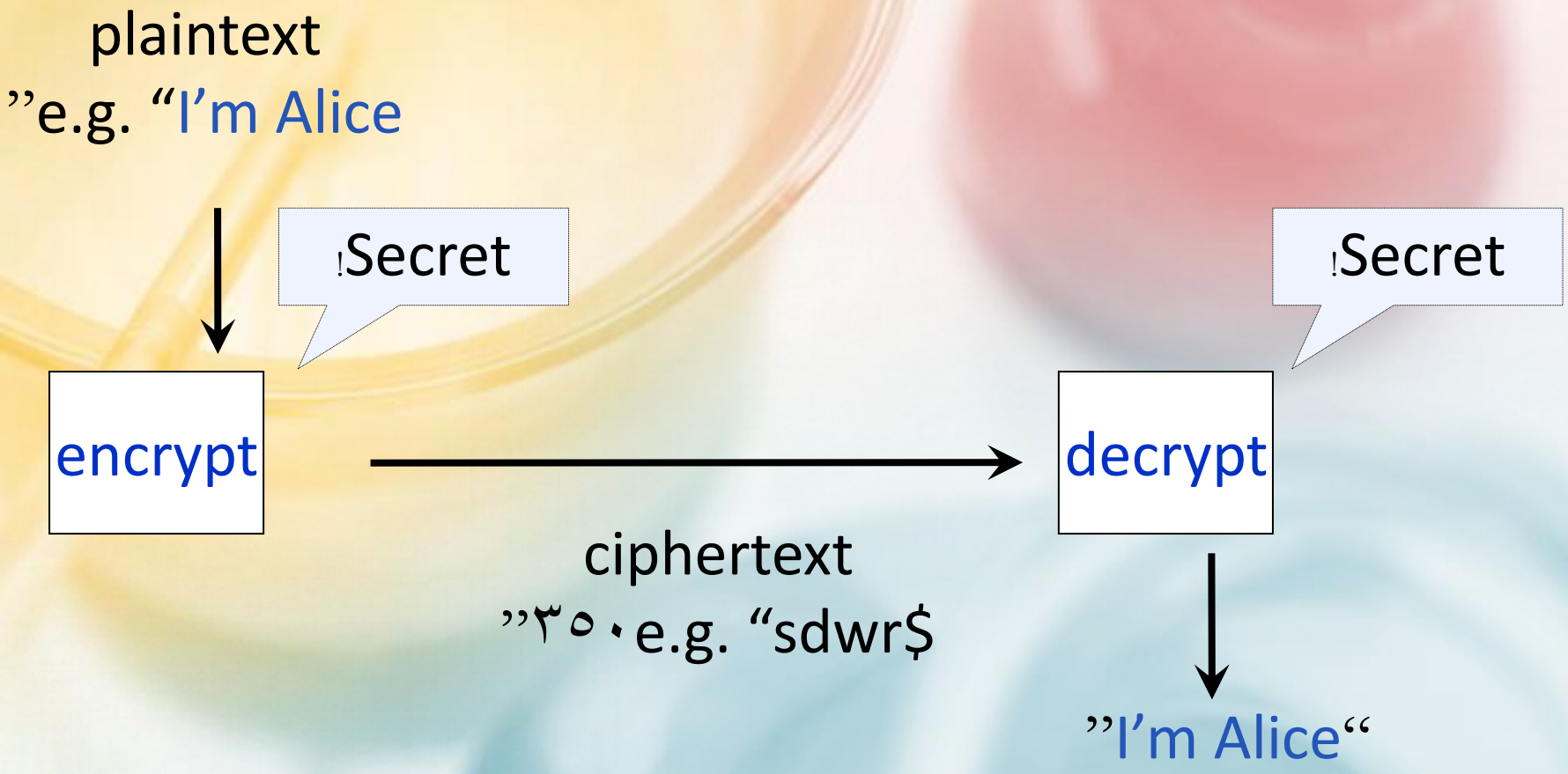
INFORMATION SECURITY

Lecture-3

Eng. Taghreed Harfoush

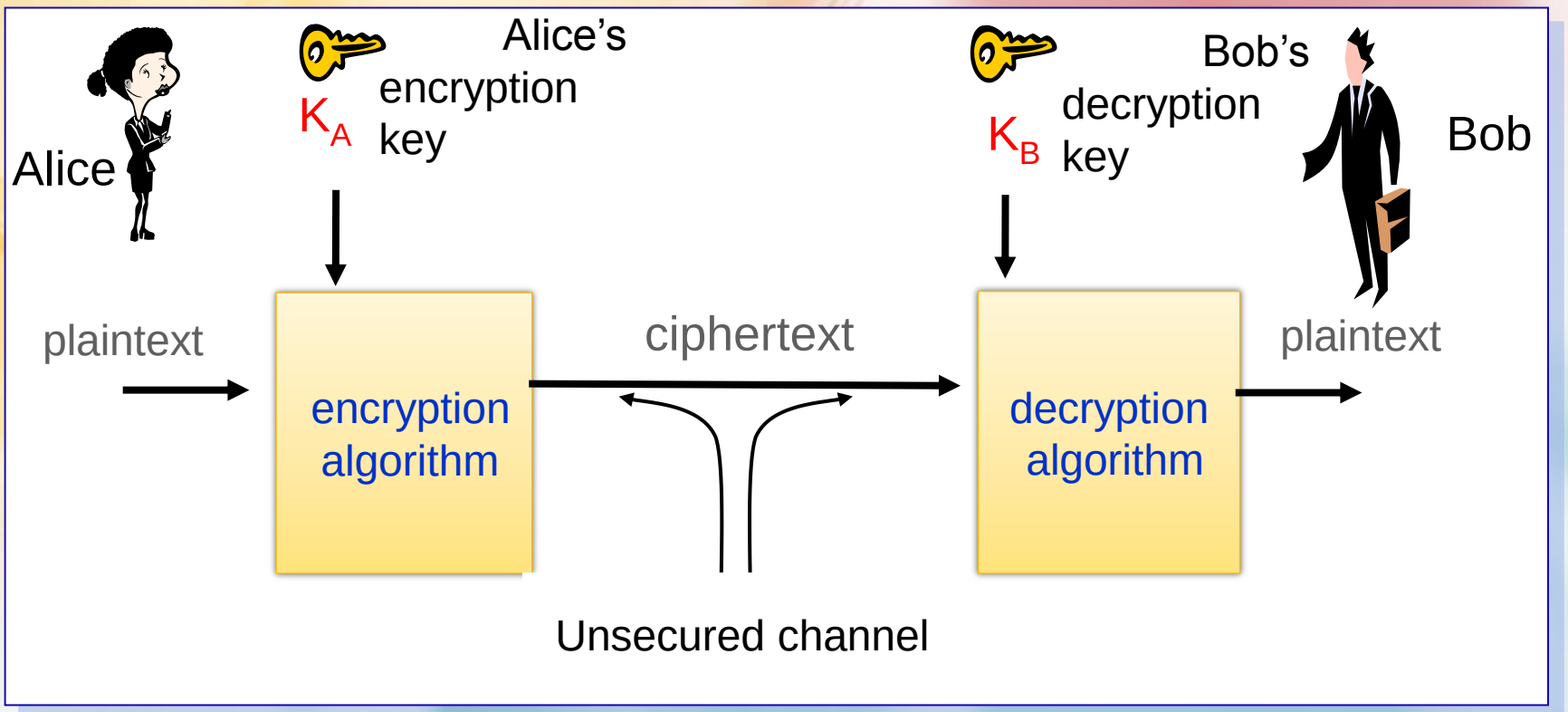
CRYPTOGRAPHY

- Greek kryptós (hidden) and gráphien (to write)
- **Cryptography** :The study of ways to hide information, or making it unreadable without secret knowledge


plaintext
”e.g. “I’m Alice
!Secret
encrypt
ciphertext
”٣٥٠e.g. “sdwr$
!Secret
decrypt
”I’m Alice“

CRYPTOGRAPHY-KEYWORDS

- **Plaintext**: This is the original message or data that is fed into the algorithm as input.
- **Ciphertext**: This is the scrambled message produced as output.
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key**: The secret key is also input to the encryption algorithm.
- **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.


Alice
Alice's
encryption
key
K_A
K_B
decryption
key
Bob's
Bob
plaintext
encryption
algorithm
ciphertext
decryption
algorithm
plaintext
Unsecured channel

CRYPTOSYSTEM

A cryptosystem is a five-tuple (M,C,K,E,D), where the following are satisfied:

- M is a finite set of possible plaintexts over an alphabet A.
- C is a finite set of possible ciphertexts over B.
- K, the keyspace, is a finite set of possible keys
- E is the encryption algorithm
- D is the decryption algorithm

For each e ∈ K there is a unique key d ∈K such that

$$D_d(E_e(m)) = m$$

ek: M → C

dk: C → M

example:

$M = (m_1, m_2, \ldots\ldots, m_n), C = (c_1, c_2, \ldots\ldots\ldots, c_n)$

$E_k(m) = (m_i + k) \bmod 26$

$D_k(c) = (c_i - k) \bmod 26$

K=3 ، m="cooz",A=0,B=1,….

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- C=((2+3 mod 26),(14+3 mod 26),(14+3 mod 26),(25+3 mod 26))

  =Frrc

CLASSIFICATION OF ENCRYPTION SCHEME

- Symmetric-key encryption
  - The sender and the receiver use the same key

$$E_K(M) = C$$

$$D_K(C) = M$$

$$D_K E_K(M) = M$$

- Asymmetric-key encryption
  - The sender and receiver use two different keys

$$E_e(M) = C$$

$$D_d(C) = M$$

$$D_d(E_e(M)) = M$$

(e,d) encryption/decryption key pairs.

CRYPTANALYSIS

Recovering a plaintext from a given ciphertext without knowing the key or recovering the key.

SECURITY LEVELS

- Unconditionally Secure
  - The ciphertext generated by the scheme does not contain enough information to determine uniquily the plaintext.
- Computationally Secure
  - Cost of breaking a ciphertext exceeds the value of the hidden information
  - The time taken to break the ciphertext exceeds the useful lifetime of the information

HISTORICAL (CLASSICAL) CRYPTOGRAPHY

- Two basic types
  - Substitution ciphers
  - Transposition (permutation) ciphers
- Product ciphers
  - Combinations of the two basic types

Q&A