Taibah University **Applied College** **Computer and Information Science** **CYBER SECURITY Program** **2nd exam (فرع)**	الكلية التطبيقية	**Code: CYB235** **Course: Basic Cryptography** **Date: 22-5-2023** **Time: 60 Min.** **Exam Model: A**

Student Name: ..... Section: ..... ID……..

PART ONE (MCQ): Choose the correct answer, and then fill the table with the chosen letter (10 Marks)

Q	1	2	3	4	5	6	7	8	9	10
ANS										

1) A secret key for symmetric encryption that is generated for use for a short period of time is called a [ ].

a) strategic key ✗ b) sequence key ✗ c) session key d) stream key → for symmetric stream encryption

2) A source that is effectively random is referred to as [ ].

a) an open source b) a keystream c) an entropy source d) a seed → must be random or pseudorandom number

3) A [ ] uses a nondeterministic (غير حتمي) source to produce randomness.

a) RC4 ✗ b) TRNG c) PRNG d) PRF

4) Two approaches that use a block cipher to build a PNRG and have gained widespread acceptance are:

a) CTR mode and CFB mode b) CTR mode and OFB mode

c) CBC mode and CFB mode d) OFB mode and ECB mode

5) If two parties use two different keys in their cryptosystem, the system is

a) Asymmetric b) Symmetric

c) One-key d) Conventional encryption

6) In RSA, the Euler Totient Function, Ø(n), is

a) private and calculated b) public and chosen

c) private and chosen d) public and calculated

7) Which of the following is correct regarding asymmetric cryptography?

a) Encryption and decryption take the same amount of time
b) The same key is used for encryption and decryption.
c) Cryptographic operations are one-way, and not reversible.
d) Different keys are used for encryption and decryption.

8) ……can be used for encryption/decryption, Digital signature, and Key exchange

a) RSA and DSS b) RSA and Diffie-Hellman

c) DSS and Diffie-Hellman d) RSA and Elliptic curve

9) DES S-box is:

a) 8-bit input & 4-bit output b) 4-bit input & 8-bit output

c) 8-bit input & 8-bit output d) 6-bit input & 4-bit output

10) [ ] effect means that a small change in either the plaintext or the key should produce a significant change in the cipher text.

a) Statistical b) Differential

c) Linear d) Avalanche

PART TWO: PROBLEM SOLVING

Q1: What is the result of passing 11010100 to the IP-box of S-DES? (1 Mark)

3	6	7	1	5	2	8	4

0 1 0 1 0 1 0 1

Q2: What is the IP^{-1}-box that corresponds to the above IP-box given in Q1? (1 Mark)

4 6 1 8 5 2 3 7

Q3: Consider the following S-Box, what is the output if the input is 111111? (1 Mark)

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

13

Q4: Suppose the input to E/P (4 1 2 3 2 3 4 1) in S-DES is 0100, then the output will be_____ (1 Mark)

0 0 1 0 1 0 0 0

Q5: Consider a S-DES with a 10-bit key (1100110010) and the following P10 and P8 tables:

P10	10	1	9	2	8	3	7	4	6	5

P8	9	3	6	1	8	2	10	7

Then, according to the key generation, the output of P8 stage (the first round sub-key K1) is: (2 Marks)

1 1 0 1 1 1 0 0

Q6: In a public-key system using RSA, you intercept the cipher text C=12 sent to a user whose decryption key is d = 5, where n=35(p=5 and q=7). The plaintext M is___17_____

---**(2 Marks)**

Q7: In a public-key system using RSA, the ciphertext C of the message M = 2 using p = 7; q = 11; and public key e = 7 is ___51_____

---**(2 Marks)**

With best wishes