Course Title: Information Security principles
Date: 15 / 09 / 2014
No. of Questions: 3 Questions
Time: 2 hours
Using Calculator (No)

University of Palestine

Final Exam
Summer 2013/2014
Total Grade: 100

InstructorName: Eng. Eman Alajrami
Student No.: _____
Student Name: _____
College Name: _____
Dep. / Specialist: _____
Using Dictionary (No)

First Question — No. of Branches (1) — 10 Marks

(A)

Put (√) or (X) for each of the following statements:

1) Often secure system failure due to a break in the key distribution scheme ( )
2) When using public key encryption the security depends on securing the public key ( )
3) Network Security measures to protect data during their transmission over a collection of interconnected networks ( )
4) Active attacks are difficult to detect because they do not involve any alteration of the data. ( )
5) Fabrication is an attack on confidentiality ( )
6) Monoalphabetic substitution ciphers do not change relative letter frequencies ( )
7) Vigenère Cipher is a Monoalphabetic substitution cipher ( )
8) Substitution cipher hide the message by rearranging the letter order without altering the actual letters used ( )
9) A substitution followed by a transposition makes a new much harder cipher ( )
10) In AES, shift rows always followed by mix columns ( )

Second Question — No. of Branches (1) — 10 Marks

(A)

Define 5 of the following briefly:

1. session key

.....
.....
.....

2. Security Attack

……
……
…….....

3. DES

.....
.....
.....

4. DSS

.....
.....
.....

5. KDC

.....
.....
.....

6. RSA

.....
.....
.....

7. Invisible watermarking

.....
.....
.....

8. Steganography

.....
.....
.....

9. MAC

.....
.....
.....

10. Fabrication

.....
.....
.....

Third Question **No. of Branches (8)** **80 Marks**

(A)

Answer Only 8 of the following questions:

1. Compare between the following pairs:

a. Block Cipher and Stream cipher

.....
.....
.....

b. AES and DES

.....
.....
.....
.....
.....
.....

c. Link encryption and end-to-end encryption

.....
.....
.....
.....
.....
.....

2. What is the purpose of using S-Boxes in DES?

.....
.....
.....
.....
.....
.....

3. Using a Playfair matrix with the key "COMMENT", encrypt this message "Session Key" ?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

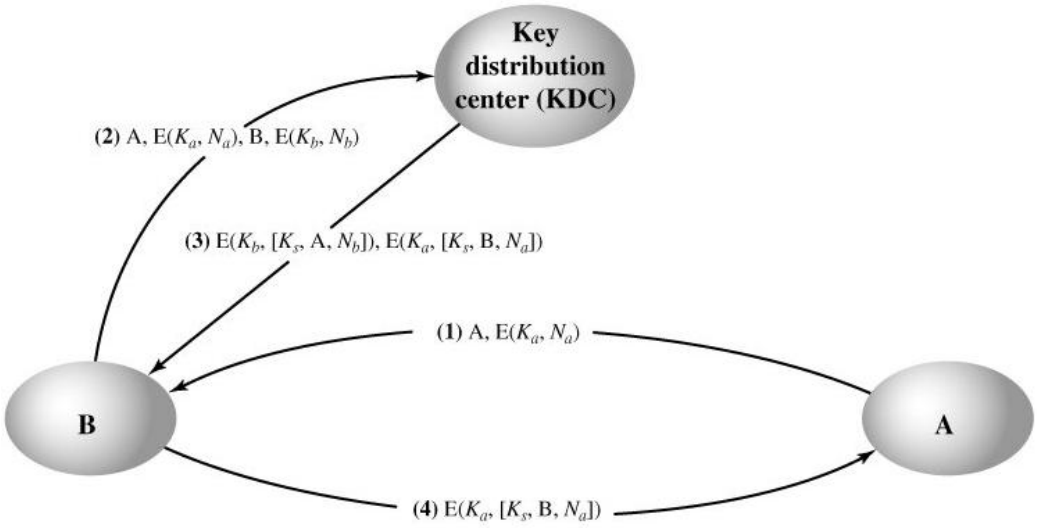
4. Explain what are the steps done in the tenth round in AES? Why they follow this arrange?

.....
.....
.....
.....
.....
.....
.....
.....
.....

5. How confidentiality and authentication can be applied in Public Encryption (RSA)?

.....
.....
.....
.....
.....
.....

6. Explain in details how the following Key Distribution Scenario work?



.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

7. What are the features of watermarking?

.....
.....
.....
.....
.....
.....
.....
.....

8. Explain how can you use Least Significant Bit method in steganography by the following example: **Data to be inserted: character '*F' and*** Host pixels: 3 pixel

   00100111 11101001 11001000
   00100111 11001000 11101001
   11001000 00100111 11101001

   How the average of the pixels actually changes from 0-1 or 1-0?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

9. Draw a chart the following:

1. **Watermarking system**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2. MAC Algorithm using public encryption.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

3. Steganography System

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Good Luck