Course Title: Information Security principles
Date: 23 / 03 / 2014
No. of Questions: 3 Questions
Time: 1 hour
Using Calculator (No)

University of Palestine

Midterm Exam
2nd semester 2013/2014
Total Grade: 20

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

First Question — No. of Branches (1) — 2.5 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) Using of automatic key distribution on behalf of users does not depend on the trust in the system ( )
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) — 2.5 Marks

(A)

Define 5 of the following briefly:

1. session key

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

2. Security Attack

……
……
…….....

3. DES

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

4. PRGNs

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

5. KDC

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

Course Title: Information Security principles
Date: 23 / 03 / 2014
No. of Questions: 3 Questions
Time: 1 hour
Using Calculator (No)

University of Palestine

Midterm Exam
2nd semester 2013/2014
Total Grade: 20

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

Third Question	**No. of Branches (7)**	**15 Marks**

(A)

Answer the following questions:

1.Compare between the following pairs:

a. Block Cipher and Stream cipher

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

b. AES and DES

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

c. monoalphabetic cipher and polyalphabetic cipher

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

d. link encryption and end-to-end encryption

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

2.What are the essential ingredients of a symmetric cipher?

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

3.Using a Playfair matrix with the key "COMMENT", encrypt this message "Session Key" then show how the decryption process will be done?

4. What is the purpose of the S-boxes in DES? How does it work? Support your answer by drawing. Using example 110011

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

6. Use Row Transposition Cipher to encrypt the message " Welcome to Information Security" With the key 32451

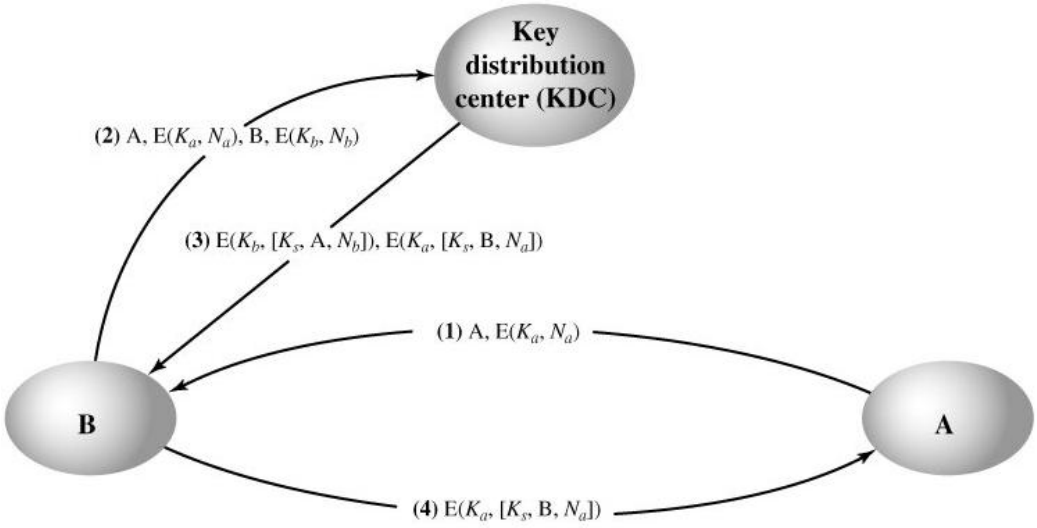
Course Title: Information Security principles
Date: 23 / 03 / 2014
No. of Questions: 3 Questions
Time: 1 hour
Using Calculator (No)

University of Palestine

Midterm Exam
2nd semester 2013/2014
Total Grade: 20

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

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



Good Luck