Course Title:Information Security Principles	**University of Palestine**	**Instructor Name: Eng.EmanAlajrami**
Date:/05/2014		**Student No.:** ________________
No. of Questions: 3 Questions	**Final Exam**	**Student Name:** ______________
Time: 2 hours	**2013/2014**	**College Name:** ______________
Using Calculator (No)	**Total Grade: 60**	**Dep. / Specialist:** ______________
		Using Dictionary (No)

First Question — No. of Branches (5) — 5 marks

Define the following:

1. **RSA**

----

2. **PGP**

----

3. **Master key**

----

4. **Firewall**

----

5. **DSS**

Second Question — No. of Branches (9) — 40 marks

Answer Only 8 questions of the following:

1.How PGP Operation for Confidentiality is done?

----

2. **Fill the following about DES**
   - **Key size: ……………………………………..**
   - **Block size: …………………………………...**
   - **Number of rounds: ………………………….**
   - **Number of S-Boxes: ………………………...**
   - **Li = …………………………………………..**
   - **Ri = …………………………………………..**

3. **In RSA if Alice and Bob want to communicate and Alice keys: private key (d) is 7 and public key (e) is 13, Bob keys: Private (d) is 3 and public key (e) is 11.**
how can they send the message " Exam" using confidentiality and authentication at the same time? (Note : the value of n is not needed just show how will they use the keys without computing the values).

4. a) 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?

b) If the host pixel are two, how can you solve the above question?

Host pixels in RGB 24 bit/pixel

00100111 11101001 11001000
11001000 00100111 11101001

5. **Fill the following about AES**
    - **Key size: ……………………………………..**
    - **Block size: …………………………………...**
    - **Number of rounds: ………………………….**
    - **Number of S-Boxes in a single round: …….**

6. **How digital signature verification can be handled?**

----

7. **How SET Transaction can be handeled?**

----

8. **Name three antivirus software?**

----

9. **Describe the types of Malicious Software? Name them.**

Third Question | **No. of Branches (3)** | **15 marks**

Draw a chart the following:

1. Watermarking system

2. **MAC Algorithm using public encryption.**

3. Steganography System

ONLY For students who didn't attend Mid Exam

1. What is the purpose of S-Boxes in DES? How does S-Boxes in DES work?

Course Title:Information Security Principles	**University of Palestine**	**Instructor Name: Eng.EmanAlajrami**
Date:/05/2014		**Student No.: ________________**
No. of Questions: 3 Questions	**Final Exam**	**Student Name: ______________**
Time: 2 hours	**2013/2014**	**College Name: ______________**
Using Calculator (No)	**Total Grade: 60**	**Dep. / Specialist: ______________**
		Using Dictionary (No)

2. Using play fair algorithm with keyword " Security" encrypt the message "balloon"

Good Luck