Course Title: Information Security Principles	**University of Palestine**	**Instructor Name: Eng. Eman Alajrami**
Date: 17/11/2013		**Student No.: _____**
No. of Questions: 2 Questions	**Midterm Exam**	**Student Name: _____**
Time: 1 hour	**1st semester 2013/2014**	**College Name: _____**
Using Calculator (Yes)	**Total Grade: 20**	**Dep. / Specialist: _____**
		Using Dictionary (No)

First Question **No. of Branches (1)** **5 matks**

Define the following:

1. **Data Integrity**

---

2. **Fabrication**

---

3. **PRNGs**

---

4. **Session key**

---

5. **Symmetric Encryption**

Second Question **No. of Branches (5)** **15 marks**

1. **What are the Key Distribution alternatives if there are two parties A and B want to communicate?**

---

2. **If palyfair matrix which is used is 25x1 how will it work? And which encryption algorithm it will be similar to?**

Course Title: Information Security Principles	**University of Palestine**	**Instructor Name: Eng. Eman Alajrami**
Date: 17/11/2013		**Student No.: _____**
No. of Questions: 2 Questions	**Midterm Exam**	**Student Name: _____**
Time: 1 hour	**1st semester 2013/2014**	**College Name: _____**
Using Calculator (Yes)	**Total Grade: 20**	**Dep. / Specialist: _____**
		Using Dictionary (No)

3. Use the Playfair matrix with the key "Welldone" to encrypt the message "It is necessary"? Show decryption how can be held?

Course Title: Information Security Principles	**University of Palestine**	**Instructor Name: Eng. Eman Alajrami**
Date: 17/11/2013		**Student No.: _____**
No. of Questions: 2 Questions	**Midterm Exam**	**Student Name: _____**
Time: 1 hour	**1st semester 2013/2014**	**College Name: _____**
Using Calculator (Yes)	**Total Grade: 20**	**Dep. / Specialist: _____**
		Using Dictionary (No)

4. What happens in each single round in DES ? Support your answer by drawing?

---

5. How sub bytes work in AES? And how the last round in AES differs from the others?

Course Title: Information Security Principles	**University of Palestine**	**Instructor Name: Eng. Eman Alajrami**
Date: 17/11/2013		**Student No.: _____**
No. of Questions: 2 Questions	**Midterm Exam**	**Student Name: _____**
Time: 1 hour	**1st semester 2013/2014**	**College Name: _____**
Using Calculator (Yes)	**Total Grade: 20**	**Dep. / Specialist: _____**
		Using Dictionary (No)

6. U**sing the keyword** ***" Server"*** **, Encrypt the following message according to Vigenère cipher**

Plain Text : " What an easy exam!"

Hint : you can use the following tables

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Good Luck