FEDERAL UNIVERSITY OF TECHNOLOGY MINNA
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY
DEPARTMENT OF INFORMATION & MEDIA TECHNOLOGY
SECOND SEMESTER EXAMINATION, 2013/2014 ACADEMIC SESSION

Course Code: *IMT 526* **Course Title:** *Computer Security Techniques*

Credit Unit: *2* **Time Allowed**: *2 ¼ Hours.*

Instruction: Answer only **three (3)** questions.

Question 1

(a) Explain the features of complexity theory that could contribute to understanding of complexities associated with information system security. (5 marks)

(b) Why is complexity theory important in the field of cryptography? (5 marks)

(c) i. State the formal definition of Euclidean algorithm for computing gcd. (2 marks)

ii. Use Euclidean algorithm to find the gcd of 393290450 and 24174444. (8 marks)

Question 2

(a) An unfair dice with four faces produced the following probability distributions of p(1) = ½ , p(2) = ¼ , p(3) = 1/8 and p(4) = 1/8 when thrown. Calculate its entropy. (8 marks)

(b) i. Discuss the envisaged contribution of Vernam's one-time pad to information security? (3 marks)

ii. Why is Vernam's one-time pad not practically achievable despite fast computing resources available nowadays? (4 marks)

(c) Explain Unicity distance. (5 marks)

Question 3

(a) Discuss how the following groups of people were able to securely keep information from unintended audience during the early age of cryptography. (6 marks)

i. Romans ii. Egyptians iii. Greeks

(b) Explain the following cryptology concepts in detail. (9 marks)

i. Monoalphabetic cipher ii. Digital signature iii. Stream cipher

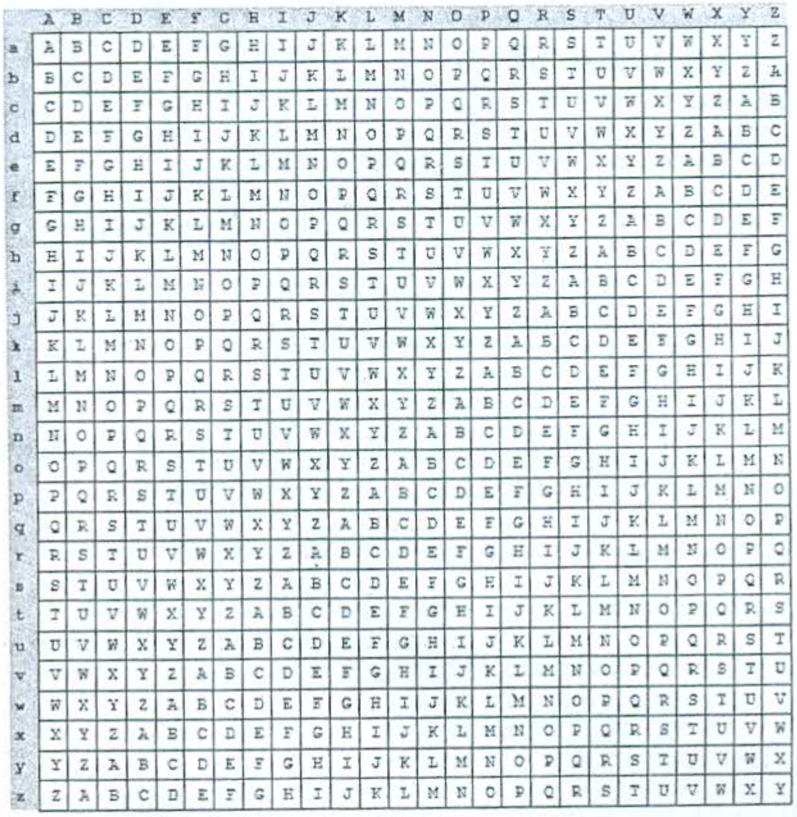
(c) List any five (5) encryption approaches employed in digital image scrambling. (5 marks)

Question 4

(a) i. Explain cryptanalysis? (5 marks)

ii. List the three generally recognized methods for cryptanalysis. (3 marks)

(b) Use autokey cipher to decrypt the ciphertext **QEZCLSKJQICBJF** with cipher key **XAZU** using Tabula Recta in Table 1. Assume the cipher key was used only once and at the beginning of the keystream during encryption. (8 marks)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 1: Tabula Recta

(c) . Explain digital image scrambling in term of information hiding. (4 marks)

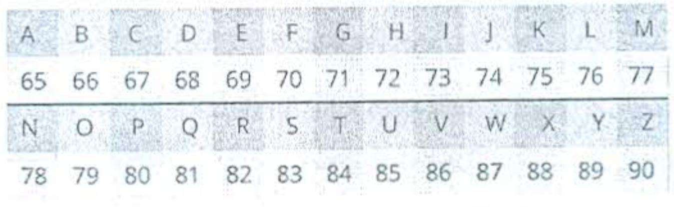
Question 5

(a) Explain threshold scheme as applicable to computer security. (5 marks)

(b) i. State the properties of an ideal hash function. (4 marks)

ii. Describe the main part of **DES** cipher using a well-structured algorithm. (3 marks)

(c) Use **RSA** parameters defined by (n: 253, e: 3, d: 147) to encrypt **NIGER**. The ASCII code is provided in Table 2. (8 marks)



A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Table 2: ASCII

Best of Luck.