KENYA METHODIST UNIVERSITY

END OF TRIMESTER EXAM APRIL 2009

FACULTY	**:**	**SCIENCES**
DEPARTMENT	**:**	**COMPUTER INFORMATION SYSTEMS**
COURSE CODE	**:**	**CISY 431**
COURSE TITLE	**:**	**INFORMATION SYSTEMS SECURITY**

Total Marks (70)

TIME: 2 HOURS

INSTRUCTIONS

Answer all questions in SECTION A and ANY TWO questions in SECTION B
The VIGENERE TABLE is attached for any relevant questions.

SECTION A – Answer ALL questions

Question 1 – 30 marks

i. Define the following terms
   a. Nonrepudiation
   b. Computationally secure
   c. Group (3 marks)

ii. Construct a Playfair matrix with the key *largest.* (4 marks)
   a. Using the Playfair matrix from **a.)** encrypt this message:

   Must see you over Cadogan West. (5 marks)

iii. Using the extended Euclid's algorithm, find the multiplicative inverse of 1234 mod 4321 (5 marks)

iv. Perform encryption and decryption using the RSA algorithm, for the following:

   a. p = 3; q = 11, e = 7; M = 5
   b. p = 17; q = 31, e = 7; M = 2. (6 marks)

v. What is the difference between a mono-alphabetic cipher and a poly-alphabetic cipher? (2 marks)

vi. Distinguish between logical security and physical security. (2 marks)

vii. List three objectives of information security. (3 marks)

SECTION B – Answer ANY TWO questions

Question 2 – 20 marks

i. Show that a Feistel decryption is the inverse of a Feistel encryption. (10 marks)

ii. Encrypt the message "**meet me",** using the Hill cipher with the key 9 4 . Show your calculations and the result. 5 7 (10 marks)

Question 3 – 20 marks

i. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? (6marks)

ii. In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe? (8 marks)

iii. Convert the plaintext "THE BUTLER DID IT" to ciphertext, using k=13 on Ceasar Cipher (6 marks)

Question 4 – 20 marks

i. Using the Vigenère cipher, encrypt the word "explanation" using the key *leg*. (4 marks)

ii. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key K and the plaintext, namely:

in hexadecimal notation: 0 1 2 3 4 5 6 7 8 9 A B C D E F

in binary notation: 0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 0100 1101 1110 1111

a. Derive K_1, the first-round subkey. (8 marks)
b. Derive L_0, R_0. (8 marks

Use the following information:

a. A bit rotation of 1
b. Permutation choice 1 for key

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

c. Permutation choice 2 for key

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

d. Initial permutation for plaintext

(a) Initial Permutation (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

VIGENERE TABLE

	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