DEDAN KIMATHI UNIVERSITY OF TECHNOLOGY

UNIVERSITY EXAMINATIONS 2021/2022 ACADEMIC YEAR

THIRD YEAR EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN BUSINESS INFORMATION TECHNOLOGY

CIT 3211: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: 2/12/2021 **TIME: 08.30-10.30 A.M.**

INSTRUCTIONS: Answer Question **ONE** and **Any** Other **Two** Questions**.** Every question should begin on a **FRESH** page and should be well labeled and **registration number should be written on every page**

QUESTION ONE: COMPULSORY (30 MARKS)

a) Paula lives in Nyeri county in Kenya, she is communicating with her friend Kevo who lives in Guangzhou City, China using electronic mail. Discuss **four** security threats that Kevo and Paula should be aware of as they communicate. [4 marks]

b) Using illustrations, explain in detail different risk control strategies. [5 marks]

c) Show how Caesar Cipher can be used to decrypt the following piece of cipher text and the resulting plain text if key 2 was used for encryption. [2 marks]

Plaintext Alphabet	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
Ciphertext Alphabet	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

Plain text - WPKXGTUKVA UVWFGPV. [3 marks]

d) Discuss five factors that determine the strength of an encryption algorithm. [5 marks]

e) Distinguish between mono-alphabetic and poly-alphabetic ciphers. Give an example of each. [2 marks]

f) The Vigenere Cipher is based on the following tableau:

	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

Show how you can encipher the plaintext message TO BE OR NOT TO BE THAT IS THE QUESTION using the key “RELATIONS". [5 marks]

g) Using illustrations, demonstrate the recommended practices in designing firewalls. [6 marks]

QUESTION TWO (20 MARKS)

a) Distinguish between **Intrusion Detection Systems(**IDS) and **Intrusion Prevention Systems (**IPS). [2 marks]

b) Discuss the different types of Intrusive Detection System (IDS). [10marks]

c) Assuming you are an ICT support staff in charge of system administration at one of local major transport Sacco. Demonstrate how Scanning and Analysis tools are useful in enforcing Computer Security. [4 marks]

d) Two different offices on campus Area Network(CAN) are working to straighten out an error in an employee’s bank account due to a direct deposit mistake. Listed below is the information flow from the “office”: -

#1, emails the correct account and deposit information to office

#2, which promptly fixes the problem. The employee confirms with the bank that everything has, indeed, been straightened out.

Discuss the security concern with this arrangement. [4 marks]

QUESTION THREE (20 MARKS)

a) Compare between Symmetric and Asymmetric encryption. [6 marks]

b) You are an employee an international organization dealing with exportation of horticultural products. You receive the following email from the help desk:
Dear XYZ Email user,
To create space for more users we're deleting all inactive email accounts. Here's what you have to send to save your account from getting deleted:
- *Name (first and last):*
- *Email Login:*
- *Password:*
- *Date of birth:*
- *Alternate email*

If we don't receive the above information from you by the end of the week, your email account will be terminated.
As a user of the services, justify what you will do. [4 marks]

c) Using the goal of "Access Confidential Information" or Access Control list(ACL) draw an attack tree or steps depicting the different ways by which an attacker could access confidential information from a home user's Windows computer. Assume no computer or network security has been implemented. [5 marks]

d) Using illustration discuss the threats faced by an information system in an Organization. [5 marks]

QUESTION FOUR (20 MARKS)

a) Algorithms can be said to be *strong* or *weak* depending on their susceptibility. In respect to this, describe the terms ***unconditionally secure*** and ***computationally infeasible***. [4 marks]

b) Describe Julius Caesar cipher algorithm and show how the following cipher can be represented in plain text. "**Duh brx uhdgb iru wkh uljruv ri wkh mre pdunhw? Brx duh vxud!** ". [4 marks]

c) Two scientists working for Atomic Energy body want to communicate some highly sensitive information using the internet infrastructure. They both have PGP and other private keys for each other. They have consulted you to explain the efficiency of each of the following options in the context of their need.

i. Transmission through plaintext. **[**2 marks]
ii. One party signs with the private key and sends to the other. [2 marks]
iii. One party signs with the public key and sends to the other. [2 marks]
iv. One party encrypts with the other public key, signs with private key and sends. [2 marks]
v. One party signs and encrypts with the shared secret key. [2 marks]

vi. Parties negotiate using Deffie Hellman for session key then encrypt using negotiate key.
[2 marks]