THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

P.O. Box 62157
00200 Nairobi - KENYA
Telephone: 891601-6
Fax: 254-20-891084
E-mail:academics@cuea.edu

MAIN EXAMINATION

MAY – JULY 2018 TRIMESTER

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND LIBRARY SCIENCE

REGULAR PROGRAMME

CMT 405: INFORMATION SYSTEMS SECURITY

Date: JULY 2018	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any other TWO Questions	

Q1. a) Define the following terms as used in security.

i) A security system **(2 Marks)**
ii) Exposure **(1 Mark)**
iii) Threats **(1 Mark)**
iv) Vulnerability **(1 Mark)**
v) Attack **(1 Mark)**
vi) Adversary **(1 Mark)**
vii) Security Control **(1 Mark)**

b) List any **six** sources of threats **(6 Marks)**

c) Differentiate between passive and active attacks. **(4 Marks)**

d) Draw a clearly labeled diagram of the access control reference monitor model. **(4Marks)**

e) Outline the principles followed during the design of secure protection systems. **(8 Marks)**

Q2. a) Viruses can be classified into various categories . Discuss any three . **(3 marks)**

b) Outline three threats posed by hackers on the Internet **(3 marks)**

c) You are an IT manager of a company. One of your roles is to ensure that your systems are secure from threats. Discuss the three most fundamental security goals that need to be addressed. **(6 Marks)**

d) Discuss the various kinds of threats to the security of a computer system **(8 Marks)**

Q3. a) Discuss the revocation methods that can be applied during authorization **(4 Marks)**

b) Define authentication and hence highlight any four personal forms of authentication that can be used. **(4 marks)**

c) Define and give examples of the following security control techniques and mechanisms categories. **(12marks)**

i) Physical security control
ii) Administrative security control
iii) Logical security control

Q4. a) Define the term Cryptography. **(2 Marks)**

b) Describe what happens in a classical substitution ciphers. **(4 Marks)**

c) Decode the following message that was coded using Caesar's cipher model. **(4 Marks)**

Show your working

FUBSWRJUDSKB LV LQWHUHVWLQS

d) Differentiate between block vs stream ciphers. **(4 Marks)**

e) List the various form of exposures to resources and information **(6 Marks)**

Q5. a) Discuss wiretapping **(4 Marks)**

b) Discuss the two major flaws in UNIX operating system. **(6 marks)**

c) Justify the security features needed for an ordinary multiprogramming operating system environment. **(10 marks)**

END