THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

P.O. Box 62157

00200 Nairobi - KENYA

Telephone: 891601-6

MAIN EXAMINATION

JANUARY – APRIL 2019 TRIMESTER

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND LIBRARY SCIENCE

REGULAR PROGRAMME

CMT 405: INFORMATION SYSTEM SECURITY

Date: APRIL 2019	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any other TWO Questions	

Q1. a) Define the terms below as they apply to security **(5 marks)**

1. Firewall
2. Denial-of-service
3. Non-repudiation
4. Front-door attack
5. Back door

b) The basis of network security, comprises of the three legs of the "security trinity triangle". Discuss the validity of these statement. In your discussion gives examples of tools and or services that may apply. **(13 marks)**

c) In order to develop your own security policy one may be required to classifying your systems and assign risk to each security entity. Discuss the significance of the Security Classification hierarchy in security policy development. **(6 marks)**

d) Explain how one can plant a back door attack program in Linux and how the system administrator can detect and hence minimize such on occurrence. **(6 marks)**

Q2. a) Define the term risk as far as information system security is concerned. **(2 marks)**

b) Discuss a comprehensive strategy one may adopt to reduce such risk as much as possible. **(8 marks)**

c) Discuss security implementations made possible by Linux passwd command. **(10 marks)**

Q3. a) Explain the meaning of the term polyalphabetic substitution cipher. **(6 marks)**

b) Consider a poly-alphabetic substitution cipher where A = {A, B, C, . . . , X, Y, Z} and t = 4. Choose e = e (p1 , p2 , p3 , p4), where p1 maps each letter to the letter two positions to its right in the alphabet, p2 to the one five positions to its right, p3 to the one seven positions to its right and p3 nine positions to its right.
If m = *STUDY OF MATHEMATICAL TECHNIQUES RELATED TO INFORMATION SECURITY,* obtain c = Ee (m) **(8 marks)**

c) Discuss the factors you may consider when creating a security policy. **(6 marks)**

Q4. a) Explain any five security requirements **(10 marks)**

b) Explain what the following symmetric cipher commands do

i) $ openssl enc -des3 -salt -in marks.doc -out ciphertext.bin **(3 marks)**

ii) $ openssl enc -des3-ede-ofb -d -in ciphertext.bin -out marks.doc -pass pass:avocado **(3 marks)**

c) Define the term Certificate as used in security **(2 marks)**

d) Write the openssl command that will create a self-signed certificate stored in the file privkey.pem **(2 marks)**

Q5. a) Explain the following concepts and with examples show how Linux implements them to enhance the security of a computer and its data.

i) I P tables **(4 marks)**
ii) Sudoers file **(4 marks)**
iii) Hash algorithm **(2marks)**

b) Define the term cryptographic hash function **(3 marks)**

c) List security applications of Cryptographic hash functions. **(7 marks)**

END