MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY ORDINARY EXAMINATION

2018/2019 ACADEMIC YEAR

THIRD YEAR **FIRST** SEMESTER EXAMINATION FOR, DIPLOMA IN CRIMINOLOGY AND SECURITY STUDIES

SCS 058 – COMPUTER SYSTEMS SECURITY

DURATION: 2 HOURS

DATE: 20/12/2018

TIME: 9:00-11:00AM

Instructions to candidates:

1. Answer question One and Any Other Two questions
2. Mobile phones are not allowed in the examination room.
3. You are not allowed to write on this examination question paper.

SECTION A: ANWER ALL QUESTIONS IN THIS SECTION

QUESTION ONE (30 MARKS)

a) Define the term cryptanalysis (1 mark)

b) What is computer system security (2 marks)

c) How does threat, attack and vulnerability relate to one another in the context of computer system security (6 marks)

d) During its lifetime, a typical virus undergoes through four main phases. Highlight the four phases (4 marks)

e) The study shows that there are no secure systems that are against attack. Therefore, risk assessment and management is the recommended practice. What do you understand by the term instinctive risk assessment (2 marks)

f) Highlight some of the common threats you are likely to encounter in a computer system (3 marks)

g) What is the difference between a worm and a virus? (2 marks)

h) Other than digital signatures, biometric system security is considered the most acceptable measures to secure our systems. However, such security measures are still prone to errors. Justify (4 marks)

i) John and Samuel are classmates, the two wants to communicate without the other classmates understanding their message. Given that the message to be communicated is HELLO, how will John implement Mono alphabetic substitution (additive) cipher to encrypt this message before sending it to Samuel, assuming that the public key is given to be 15? (6 marks)

SECTION B – ANSWER ANY TWO QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Discuss any five main cyber crime preventive tips (10 marks)

b) Explain the two broad classifications of cryptography algorithms (4 marks)

c) The Data Encryption Standard (DES) is the most popular and officially accepted standard, using a well labeled diagram, give the overview of DES (6 marks)

QUESTION THREE (20 MARKS)

a) Describe the five main principles of security (10 marks)

b) Block ciphers encrypts a group of plaintexts symbols as one block. Highlight pros and cons of using this algorithm (4 marks)

c) Explain the three properties of "trustworthy" encryption systems (6 marks)

QUESTION FOUR (20 MARKS)

a) Explain the two groups of attacks in a security system (4 marks)

b) Give the difference between the following substitution ciphers: (4 marks)

    i. Mono alphabetic

    ii. Poly alphabetic

c) Given the plain text (p): ATTACK and public key (k) = 12, use poly alphabetic substitution cipher canto key cipher to decrypt this plain text to get the correct corresponding cipher text (c) (6 marks)

d) Computer crime is hard to define; yes or no? justify your answer (6 marks)