MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2017/2018

THIRD YEAR SPECIAL/SUPPLEMENTARY EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE

CCS 3475: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: SEPTEMBER 2018 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE (30 MARKS)

a) Discuss how the following access control mechanisms and their importance in computer security (9 marks)

   i. Access control lists (2 marks)

   ii. Capability lists (2 marks)

   iii. Access control matrices (2 marks)

b) Encrypt the message "welcome home" using the Hill cipher with the $\begin{bmatrix} 8 & 2 \\ 5 & 5 \end{bmatrix}$ show your calculations and the result (5 marks)

c) Cite examples from real life, where the following security objectives are needed

   Confidentiality

   Integrity

   Non-repudiation

   Suggest suitable security mechanisms to achieve them (6 marks)

d) Draw and discuss a conventional Encryption Mode (4 marks)

e) With the aid of examples differentiate between a passive and active attack (4 marks)

f) Discuss the differences between a Monoalphabetic cipher and a polyalphabetic cipher (5 marks)

QUESTION TWO (20 MARKS)

a) Explain five firewall design goals (10 marks)
b) Differentiate a security plan from a security policy (5 marks)
c) State the five services that constitutes to the actual operation of PGP (5 marks)
What is the major function of IP sec?

QUESTION THREE (20 MARKS)

a) What is the difference between a block cipher and a stream cipher? (4 marks)
b) Discuss any two limitations of firewalls (4 marks)
c) Discuss how PGP authentication works (4 marks)
d) Explain the following terms as used in ISS (8 marks)
   I. Phishing
   II. Sniffing
   III. Cryptanalysis
   IV. Cryptography

QUESTION FOUR (20 MARKS)

a) Discuss how the following access control mechanisms work. For each, state any benefits of implementing them
   i. Access control lists (3 marks)
   ii. Capability lists (3 marks)
   iii. Role based access control (3 marks)
b) Discuss three goals of a security policy (6 marks)
c) What is the difference between an unconditionally secure cipher and a computationally secure cipher? (5 marks)

QUESTION FIVE (20 MARKS)

a) What are the essential ingredients of a symmetric cipher (6 marks)

b) Given key: 4 3 1 2 5 6 7 using rail fence show how you can encrypt the message “attack postponed till two AM” (6 marks)

c) Identify four types of keys used by PGP (4 marks)

d) Given ciphertext brute-force cryptanalysis is easily performed on Caeser Cipher. Show how this problem can be solved (4 marks)