



# 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](mailto:info@must.ac.ke) Email: [info@must.ac.ke](mailto:info@must.ac.ke)

---

## University Examinations 2017/2018

### FOURTH YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF INFORMATION SCIENCE

#### CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: SEPTEMBER 2018

TIME: 2 HOURS

---

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

---

#### QUESTION ONE (30 MARKS)

- a) Using the key given use hill cipher algorithm to encrypt the message extraordinary

(9 marks)

$$\text{Key} = \begin{bmatrix} 9 & 3 \\ 2 & 11 \end{bmatrix}$$

- b) Discuss the following terms as used in computer

(6 marks)

- i. Computer security
- ii. Threat
- iii. Vulnerability

- c) Most practicing security professional confess that information security management is a challenging field. Critic the above statement giving your own views

(6 marks)

- d) Explain what a firewall is and briefly explain any two types of firewall

(3 marks)

- e) An *operating system* (sometimes abbreviated as “OS”) is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications or application programs. By

managing other programs and I/O accessibility, it means that the OS can form first line defense in your computer

Giving examples, discuss the following security provided by computer operating systems (6 marks)

- i. Discretionary Access Control (DAC)
- ii. Mandatory Access Control (MAC)
- iii. Role Based Access (RBA)

### QUESTION TWO (20MARKS)

- a) Discuss the principal elements of a public-key cryptosystem (10 marks)
- b) What are fundamental properties of a good cryptography system (6 marks)
- c) Differentiate between active and passive wiretapping (4 marks)

### QUESTION THREE (20 MARKS)

- a) Mona has been invited for interviews for the opening in the systems department in a local bank. Before the interviews, Mona and other candidates are taken through the banks systems for familiarity. Why shouldn't you show a prospective employee secure areas during interviews? Discuss three reasons (6 marks)
- b) Discuss how the following are used to ensure security of computer resources. Access control Matrix, Access Control List, Capability (9 marks)
- c) Discuss the concepts of *intrusion prevention* and *detection* (4 marks)
- d) In the old adage they say that an ounce of prevention is worth a pound of cure. Relate this statement to the importance of disaster preparedness in an organization (1 mark)

### QUESTION FOUR (20 MARKS)

- a) Explain the difference between Host intrusion detection systems and network intrusion detection systems (4 marks)
- b) Use the expression  $E(x) = (9x + 5) \text{MOD} 26$  to encrypt the message "The game has been postponed" (10 marks)
- c) Discuss the following intrusion detection methods (6 marks)
  - i. HIDS
  - ii. Signature Based
  - iii. Anomaly Based

**QUESTION FIVE (20 MARKS)**

- a) What do you understand by Denial of service attack? (2 marks)
- b) Give two reasons that support the need for the need to understand computer security by all computer users in an organization (2 marks)
- c) Discuss the two types of firewalls (4 marks)
- d) Discuss some of the physical security controls used to protect information systems in an organization (4 marks)
- e) What makes a good security policy? (4 marks)
- f) Discuss the differences between Monoalphabetic and polyalphabetic Ciphers (4 marks)