MURANG'A UNIVERSITY COLLEGE

University Examinations 2015/2016

FOURTH YEAR **FIRST** SEMESTER EXAMINATION FOR THE DEGREE OF

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

BIT 2317 : FUNDAMENTALS OF COMPUTER SECURITY

COURSE: B.Sc. IT   **TIME: 2HRS**

DAY/TIME: Monday 2.00 am   **DATE: 14/12/15**

Instructions: Answer Question 1 and Any Other Two.

Question 1: (30 Marks)

a) Define the following terms as used in computer security   (5 Marks)

       i. Cryptography

      ii. Plaintext

     iii. Cipher text

     iv. Cryptanalysis

      v. Cryptology

b) State **three** reasons why physical security is needed.   (3 Marks)

c) Biometric measurements or personal attributes are used for authentication. These attributes are unique to the individual seeking to authenticate identification.

       i. List any four types of biometrics that are used for authentication   (2 Marks)

      ii. Discuss the two types of errors that occur when biometrics are used for authentication.   (4 Marks)

d) Discuss the following block cipher encryption modes used in symmetric keys

       i. ECB   (4 Marks)

      ii. CBC   (4 Marks)

e) One of the most common attacks on corporate systems is denial of service (DoS) attacks. Briefly describe the following DoS attacks   (8 Marks)

       i. TCP SYN flood attack

      ii. Smurf IP attack

     iii. UDP flood attack

     iv. Ping of Death

Question 2: (20 Marks)

a) With use of examples discuss the three goals of security   (6 Marks)

b) Access control is a fundamental concept in computer security. Differentiate between the following access control models as used by current systems   (4 Marks)

      i.   Capability based model and

      ii.   ACL-based model

c) Discuss the four phases a typical virus goes through   (8 Marks)

d) Differentiate between authentication and authorization in relation to computer security.

                                      (2 Marks)

Question 3: (20 Marks)

a) In any given organizational setting a dedicated firewall would be required between your network and outside world. Briefly describe the different firewall configurations.

                                      (8 Marks)

b) With aid of a diagram discuss the various steps for security risk management

                                      (9 Marks)

c) Pre-emptive techniques have been widely deployed to reduce chances of successful attack. Briefly describe intrusion deflection, infiltration and intrusion deterrence techniques.   (3 Marks)

Question 4: (20 Marks)

a) Discuss the following access control

      i.   DAC   (3 Marks)

      ii.   MAC   (3 Marks)

      iii. RBAC   (3 Marks)

b) Explain briefly how XOR and Initialization vectors are used in symmetric key cryptography.   (2 Marks)

c) Security policies define how an organization deals with security aspects. With use of examples differentiate between user policies and system administration policies.

                                        (4 Marks)

  d) Describe how e-commerce sites implement asymmetric algorithm to securely perform transactions.   (5 Marks)///