TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR:

FUNDAMENTALS TO COMPUTER SECURITY

UNIT CODE: EIT 2208

END OF SEMESTER EXAMINATION

SERIES: AUGUST2019

TIME: 2HOURS

DATE: Pick DateAug2019

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of **FIVE** questions. Attemptany THREE questions.

Do not write on the question paper.

Question ONE

a) Explain the following terms in computer security [10marks]

   i. Cryptography
   ii. Cryptanalysis
   iii. Digital signature
   iv. Digital certificate
   v. Certificate authority

b) Explain two types of encryption [4marks]

c) Discuss the strengths and weaknesses of (b) above [6marks]

Question TWO

a) Briefly describe the processes of encryption and decryption in relation to cryptography

[6marks]

b) Explain the term vulnerability in the context of computer security and provide THREE (3) examples of vulnerabilities in security. [6marks]

c) Anti-virus software is commonly used to detect and prevent potential harmful attacks on a computer. With respect to the detection element of an anti-virus program, how does the antivirus program work and how do virus writers try to exploit the way these programs typically work in order to avoid detection? [6marks]

d) Discuss the range of security measures that you would recommend to improve the security of a home PC [2marks]

Question THREE

a) Security management must manage risks in terms of causes, effects and costs of a security loss.

b) The costs resulting from a security fault must be balanced with the costs resulting from enhanced security measures, since too much security wastes money while too little security wastes IS capability. Explain the following distinct stages in security management. [12marks]

i. ***Risk Identification.***
ii. ***Risk Analysis or Assessment.***
iii. ***Risk Handling***
iv. ***Disaster Recovery***

c) Explain four network attacks and security measures that can be used to mitigate those [8marks]

Question FOUR

a) Explain the functionality of a digital signature and describe how it is generated. [6marks]

b) Given the plain text**: it is hidden under the tree** is encrypted using a Caesar cipher with a shift of 3 mod 26, give the equivalent cipher text [2marks]

c) Identify and discuss the issues that would need to be considered when determining a suitable backup strategy for a medium to large organization [6marks]

d) Explain why data encryption standard is preferred than **Caesar's Cipher algorithm [2marks]**

e) Explain the term firewall in network security and discuss how it is used in network architectures. [4marks]

Question FIVE

a) Briefly describe the following encryption algorithms [12marks]

i. RSA algorithm

ii. DES algorithm

iii. Triple DES algorithm

iv. Caesar's Cipher algorithm

b) Briefly explain the key generation in RSA algorithm [4marks]

c) Firewalls use Access Control Lists (ACL). Explain what is meant by an ACL and typical contents. [4marks]