TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

Select department

UNIVERSITY EXAMINATION FOR:

DICT/JAN/2018

EIT 2208: FUNDAMENTALS TO COMPUTER SECURITY

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) Define computer security [2marks]

b) Explain three objectives of computer security [6marks]

c) Explain the following network attacks [6marks]

   i. IP Spoofing

   ii. Denial of service

   iii. Phishing

d) Differentiate between substitution and transposition encryption techniques [4marks]

e) Explain the significance of conducting risk analysis in an organization [2marks]

Question TWO

a) Define encryption [2mark]

b) Explain the following encryption algorithms [8marks]

i. RSA algorithm
ii. DES algorithm
iii. Triple DES algorithm
iv. Caesar's Cipher algorithm

c) Discuss the strengths and weaknesses of symmetric and asymmetric encryption [6marks]

d) Describe the functionality of digital signatures. [4marks]

Question THREE

a) Explain five ways of mitigating threats to computer security. [10marks]

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

c) 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. [8marks]

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

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

Question FOUR

a) Briefly describe the processes of encryption and decryption in relation to cryptograph [4marks]

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

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. [4marks]

d) Define access control lists and capabilities, and discuss their relative strengths and weakness [4marks]

Question FIVE

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

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

b) Explain World Wide Web authentication [3marks]

c) State the importance of secure electronic transaction (SET) protocol [3marks]

d) Given the plain text**: today is Monday** is encrypted using a Caesar cipher with a shift of 3 mod 26, give the equivalent cipher text [4marks]