TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

UNIVERSITY EXAMINATION FOR:

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

BIT 2317 : FUNDAMENTALS OF COMPUTER SECURITY

END OF SEMESTER EXAMINATION

SERIES: DECEMBER 2016

TIME: 2 HOURS

DATE : DECEMBER 2016

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of **five** questions. QUSTION ONE is Compulsory. Attempt any other TWO questions

Do not write on the question paper.

Question ONE

a) Explain the difference between the following terms:

i) Firewall and Intrusion Detection System (IDS)

ii) Stream cipher and Block cipher

iii) Computer security and Network Security

IV) Cryptography and Steganography

v) Hot site facility and Cold site facility **(20 MARKS)**

b) Describe any five Characteristics of a Good Security Policy **(10 Marks)**

Question TWO

a) Explain the concepts of computer security terms:

i) Confidentiality

ii) Availability
iii) Integrity **(6 MARKS)**

b) Explain the difference between
i) "security plan" and "security policy"
ii) "Network based attacks" and "Application based attacks" **(12 MARKS)**
c) Using a two rail fence cipher encrypt the message: "meet me after the toga party" **(2MARKS)**

Question THREE
a) Explain the difference between "Cryptanalysis" and "Brute-force attack" **(4 Marks)**

b) Using a well labelled diagram, describe the ingredients of asymmetric encryption (**12 Marks)**
c) Using Caesar cipher (Key = +3), decrypt the message: PHHW PH DIWHU WKH WRJD SDUWB
(4 MARKS)

Question FOUR
a) Using suitable examples describe the following attacks as identified in Risk Based Attack Taxonomy.
i) External information theft
ii) External abuse of resources
iii) External masquerading
iv Pest programs
iv) Bypassing of internal controls **(8 MARKS)**

b) Describe any four Methods of Defense used in securing information assets **(8 Marks)**
c) Define the terms:
i) Digital signature
ii) Digital signature scheme **(2 Marks)**

Question 5
a) Security management must manage risks in terms of causes, effects and costs of a security loss. The costs resulting from a security fault must be balanced with the costs resulting from enhanced security measures. This means that systematic security management allows counter-measures to be chosen in a planned and managed way, since too much security wastes money while too little security wastes Information System resources (IS) capability.
Required
Describe the four distinct stages of management of security **(16 Marks)**

b) Explain the four properties of digital signatures **(4 Marks)**