TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

Select department

UNIVERSITY EXAMINATION FOR:

BACHELOR OF TECHNOLOGY IN INFORMATION AND COMMUNICATION TECHNOLOGY

EIT 4414: CRYPTOGRAPHY AND NETWORK SECURITY

END OF SEMESTER EXAMINATION

SERIES:APRIL2016

TIME:2HOURS

DATE: Pick DateMay2016

Instructions to Candidates
You should have the following for this examination
-*Answer Booklet, examination pass and student ID*
This paper consists of **FIVE** questions. Attemptquestion ONE (Compulsory) and any other TWO questions.
Do not write on the question paper.

Question ONE

a) Using a well labelled diagrams, explain five components of a symmetric encryption scheme. (12 Marks)

b) Explain the following terms:

i) Message Digest

ii) Kerberos

iii) A digital signature (6 Marks)

c) Explain the difference between the following terms:

i) Steganography and cryptography

ii) Chinese remainder theorem and Euler's theorem (8 Marks)

d) Using Rail Fence method, encipher the statement: MEET ME AFTER THE EXAMINATION (2 Marks)

e) Using Caesar cipher (key = +3) encrypt the message: ATTACK POSTPONED UNTIL TWO AM (2 Marks)

Question TWO

a) Explain the "OSI Security Architecture" (2 Marks)
b Using suitable examples, differentiate between "Passive attacks" and "Active attacks " (6 Marks)

c) Explain the following security services:
i) Authentication
ii) Access control
iii) Data confidentiality
iv) Data integrity
v) Nonrepudiation
vi) Availability service (12 Marks)

Question THREE

a) Explain the difference between the following terms:

i) Stream cipher and block cipher

ii) Diffusion and Confusion (8 Marks)

c) State any four properties of digital signatures (4 Marks)

ii) There are four general means of authenticating a user's identity, which can be used alone or in combination. Describe these four means. (8 Marks)

Question FOUR

a) Explain the following terms:

i) Secure/Multipurpose Internet Mail Extension (S/MIME)

ii) Pretty Good Privacy (PGP)

iii) Firewall

iv) Intrusion Detection System (IDS) (8 Marks)

b) Distinguish between "Secure Shell (SSL)" and "Transport Layer Security (TLS)" (8 Marks)

c) State any four techniques historically used in steganography (4 Marks)

Question FIVE

a) Explain the difference between

i) “Substitution Cipher” and “Transposition Cipher”

ii) “Web security” and “IP Security” (8 Marks)

b) Outline any four applications of IPSEC (8 Marks)

c) using columnar method, encode the message: THE QUICK BROWN FOX JUMPS OVER LAZY DOG (4 Marks)