MERU UNIVERSITY COLLEGE OF SCIENCE & TECHNOLOGY
P.O. Box 972-60200 Meru - Kenya. Tel: 020-2092048, 020 2069349
Fax: 020-8027449

University Examinations 2012/2013

THIRD YEAR, SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUER TECHNOLOGY

BCT 2314: CRYPOGRAPHY AND COMPUTER SECURITY

DATE: DECEMBER 2012 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions*

QUESTION ONE – 30 MARKS

a. In the context of cryptography, please explain the concepts of confusion, diffusion and the avalanche effect. (6 Marks)
b. Explain how three different cryptographic techniques can be used to build a digital envelope and digital signature thus achieving secure communications. Illustrate your answer with a figure and explain how data integrity, confidentiality/privacy, authentication and non-repudiation are achieved. (7 Marks)
c. In the context of **S/MIME:**
   i. Define the following terms: **Enveloped data; signed data; clear signed data; signed and enveloped data.** (4 Marks)
   ii. Describe how an **enveloped data MIME entity** is generated. (3 Marks)
d. Alice has just learnt about IPSec and she thinks its implementation will be beneficial for her company. Help Alice prepare a brief for her superiors.:
   i. Describe **IPSec:** what it is; what is it used for; giving two examples: (5 Marks)
   ii. What are the advantages of **IPSec?** (2 Marks)
   iii. Explain **three** main functional area of **IPSec.** (3 Marks)

QUESTION TWO – 20 MARKS

a. The context of secure transmissions and cryptography, what is the importance of **Trust.** (2 Marks)
b. Briefly explain the three different trust models. (6 Marks)
c. With the help of a diagram, explain the verberos authentication scheme. (12 Marks)

QUESTION THREE – 20 MARKS

a. Describe the main properties of the Data Encryption Standard (DES). What type of an algorithm is it? What is it used for? (4 Marks)
b. What are the length of the key and the size of the block that this algorithm uses? (2 Marks)
c. With the aid of a diagram, explain its overall operational steps (or basic steps). Your answer should describe the initial and final operations as well as the operations that are repeated at each round, without giving going into the specific details on how these operations are actually performed. (8 Marks)
d. What are **S-Boxes** and what role do they perform? (2 Marks)
e. List the different techniques that have been proposed to strengthen DES. (4 Marks)

QUESTION FOUR – 20 MARKS

a. Explain each of the following types of so-called malicious software: **backdoors, logic bombs, trojan horses, zombies and worms.** (10 Marks)
b. Describe five different types of viruses. (5 Marks)
c. List and discuss three ways in which firewalls ensure network security. (5 Marks)

QUESTION FIVE – 20 MARKS

As a Network Administrator in a newly setup medium sized company you have been requested to prepare a report to your CIO outlining the measures that you would employ to implement password protection within the company.

a. User education (4 Marks)
b. Reactive measures (4 Marks)
c. Proactive measures (4 Marks)
d. Define distributed denial of service attacks (DDOS) (3 Marks)