# KENYA METHODIST UNIVERSITY

## END OF 2ND TRIMESTER 2010 EXAMINATIONS

| | | |
|---|---|---|
| **FACULTY** | **:** | **SCIENCE AND TECHNOLOGY** |
| **DEPARTMENT** | **:** | **COMPUTER SCIENCE & BUSINESS INFORMATION** |
| **UNIT CODE** | **:** | **CISY 431/BBIT 422** |
| **UNIT TITLE** | **:** | **INFORMATION SYSTEMS SECURITY** |
| **TIME** | **:** | **2 HOURS** |

***Instructions:*** Answer Question **one** and any other **two** questions.

**Question 1 (30 Mks)** Compulsory

a. Explain the following as used in ISS: -
   i. Brute force
   ii. Malware
   iii. cryptanalysis,
   iv. Spoofing
   v. Message digest [5 MKS]

b. If you had to both encrypt and compress data during transmission, which would you do first, and why? [3 MKS]

c. Give and explain the conditions for Shannon's theory for perfect security. [4 MKS]

d. Confusion is a way of hiding the relationship between statistics of cipher text. Use an XOR example to show how this can be achieved. [3 MKS]

e. Both IPSec and SSL are primarily encryption and authentication technologies for data in transit.
   i. Give any three benefits of IPSec and
   ii. Any two drawbacks of SSL. [5 MKS]

f. Using Euclid's algorithm, find the gcd (160, 940). [2 MKS]

g. Briefly explain the Deffie-Hellman key exchange. [4 MKS]

h. How are password systems designed to increase protection [4 MKS]

**Question 2 (15 Marks)**

a. The following message was encrypted with the Hill cipher using this matrix: [7 MKS]

   5 2

   2 4

   Encrypt this message.

   THE FAULT.

b. Use a diagram to explain the working principle of Feistel cipher structure given a plain text block of length 2w bits is input. [5 MKS]

c. Public key algorithms have requirements, give and explain three. [6 MKS]

d. Using a table, show how a reversible block cipher transformation with n=2 will look like? [2 MKS]

**Question 3 (15 Marks)**

a. Antiviruses have three approaches of dealing with viruses. Explain these approaches. [3 MKS]
b. What do you think is the motivation of hackers? [5 MKS]
c. What factors would be considered when implementing symmetric key encryption? [4 MKS]
d. Any web security strategy must take care of four aspects: - Integrity, Confidentiality, DOS and Authentication. What do you understand by these terms? [4 MKS]
e. DES has a strong avalanche effect. Explain what you understand by this statement. [2 MKS]
f. Give and explain any two types of firewalls [2 MKS]

**Question 4 (15 Marks)**

a. What do you think are the qualities of a strong password? [4 MKS]
b. Cryptography requires generation of random numbers. Certain mathematical criteria must be met. Define three criteria. [3 MKS]
c. Explain the working principle of the following:- [6 MKS]
    i. Secure Electronic Transfer (SET)
    ii. Certificate Authority (CA)
d. Using an example, explain how a virus infects a file. [3 MKS]
e. Why are security audits and penetration testing done?
f. Who would you recommend to do penetration testing? Why? [4 MKS]

**CISY 431 Information Systems Security**

**Course Purpose:**

The course introduces the student to information security issues and basic applications to implement security.

**Course Objectives:**

At the end of this course, the student should have:

- Understood the threats to information systems and how they are prevented.
- Understood different security approaches and their limitations.
- Carried out a programming project.

**Course Content:**

Encryption Techniques. Block Cipher Principle and the Data Encryption Standard. Modular arithmetic, Euclid's Algorithm. Advanced Encryption Standard. Random Number Generation. Principles Public-Key Cryptosystems and RSA algorithm. Key Management – Diffie Hellman Key Exchange. Digital Signatures. Authentification Applications – Kerberos. Web Security. Intruders. Malicious Software. Firewalls- Prereq. CISY 231.