THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

P.O. Box 62157
00200 Nairobi - KENYA
Telephone: 891601-6
Fax: 254-20-891084
E-mail:academics@cuea.edu

MAIN EXAMINATION

JANUARY – APRIL 2015 TRIMESTER

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

REGULAR PROGRAMME

CMT 405: INFORMATION SYSTEMS SECURITY

Date: APRIL 2015	**Duration: 2 Hours**
Instructions: Answer Question ONE and any other TWO Questions.	

Q1. a) Briefly define the following terms as used in information security;

i) Cryptography **(1 mark)**
ii) Authentication **(1 mark)**
iii) Access Control **(1 mark)**
iv) Risk management **(1 mark)**

b) Describe four reasons why it is important to have limited crypto period for keys.

(4 marks)

c) Identify the four basic properties of hash functions.

(4 marks)

d) Describe the following categories of user authentication giving an example of each.

i) Knowledge – based **(2 marks)**
ii) Object-based **(2 marks)**
iii) ID-based **(2 marks)**
iv) Location-based **(2 marks)**

e) List the three phases of access control.

(4 marks)

f) A possible definition of risk is: risk = likelihood x consequence. Briefly explain what is meant by likelihood and consequence in this definition.

(4 marks)

g) Identify the three common methods of risk avoidance.

(3 marks)

Q2. a) List four possible solutions to the problems associated with using passwords in the clear.

(4 marks)

b) Identify and describe three practical considerations when choosing a biometric.

(4 marks)

c) Briefly describe the following two classifications of biometric types giving an example of each.

i) Stable **(2 marks)**

ii) Alterable **(2 marks)**

d) Name the three types of risk analysis.

(3 marks)

e) A qualitative risk analysis has identified three levels of likelihood (low, medium, high) and three levels of consequences (minor, moderate, major). Draw an appropriate table showing the qualitative level of risk taken from five levels (negligible risk, low risk, moderate risk, high risk, extreme risk).

(6 marks)

Q3. a) Distinguish between the following terms:

i) Encoding and encryption **(2 marks)**

ii) Symmetric and asymmetric cipher **(2 marks)**

b) The Diffie-Hellman key exchange is to be used to establish a shared secret key between Alice and Bob. Alice and Bob have agreed to use the prime P = 47 and base value g =5.

i) If Alice chooses the random value a = 18, what value does Alice send to Bob? **(3 marks)**

ii) If Alice receives the value 28 from Bob, what is the value of the shared secret key? **(3 marks)**

c) Explain the major limitation of HTTP basic authentication and how this limitation is overcome in HTTP Digest Authentication. **(2 marks)**

d) Describe the following FOUR security services that can be provided by IPSec(Internet Protocol Security)

i) Message confidentiality **(2 marks)**

ii) Traffic Analysis protection **(2 marks)**

iii) Message integrity **(2 marks)**

iv) Message replay protection **(2 marks)**

Q4. a) The key compromise recovery plan should contain three major items. List them.

(3 marks)

b) Briefly describe three ways you can use to distribute a session key.

(3 marks)

c) Describe the following key management phases;
   i) Pre-operational **(1 mark)**
   ii) Operational **(1 mark)**
   iii) Post operational **(1 mark)**
   iv) Destroyed **(1 mark)**

d) Explain the following types of firewall technology
   i) Simple packet filters **(2 marks)**
   ii) Stateful packet filters **(2 marks)**
   iii) Application Gateways **(2 marks)**
   iv) Circuit level Gateways **(2 marks)**

e) Describe two problems associated with network based intrusion detection system (IDS).

(2 marks)

Q5. a) Briefly describe the following three security properties maintained in each state of a system where Bell-Lapadula security model is applied.
   i) Simple security property (ss) **(2 marks)**
   ii) Star property (*) **(2 marks)**
   iii) Discretionary security property (ds) **(2 marks)**

b) In the Bell-Lapadula security model, security labels that are assigned to subjects and objects consist of two components. List them.

(2 marks)

c) Identify the four phases that a virus and a worm go through.

(4 marks)

d) i) What is a botnet?

(2 marks)

ii) Describe two attacks that can be executed with botnets.

(2 marks)

iii) Briefly explain any four limitations of reusable passwords.

(4 marks)

END