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

AUGUST – DECEMBER 2018 TRIMESTER

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND LIBRARY SCIENCE

REGULAR PROGRAMME

CMT 405: INFORMATION SYSTEMS SECURITY

Date: DECEMBER 2018	**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) Encryption **(1 mark)**
- ii) Public Key Infrastructure **(1 mark)**
- iii) Biometrics **(1 mark)**
- iv) Business Continuity Plan **(1 mark)**

b) Describe four reasons why it is important to have limited crypto period for keys. **(4 marks)**

c) A basic biometric system consists of four modules. List them. **(4 marks)**

d) Briefly define the following approaches to access control;
- i) Discretionary access control **(2 marks)**
- ii) Mandatory access control **(2 marks)**
- iii) Role-based access control **(2 marks)**

e) Explain the term “conflict of interest’ as used in the Brewer-Nash Chinese wall security model. **(2 marks)**

f) A possible definition of risk is: risk = likelihood x consequence. Briefly explain what is meant by likelihood and consequences in this definition. **(4 marks)**

g) Identify the four basic properties of hash functions. **(4 marks)**

h) Briefly describe the four step process of generating a digital certificate. **(2 marks)**

Q2. a) 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 g = 5.

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

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

b) Briefly describe the following three security services that cryptography provides:

i) Confidentiality **(1 mark)**
ii) Integrity **(1 mark)**
iii) Authentication **(1 mark)**

c) Describe the roles of the following network related protocols:

i) HTTP authentication **(1 mark)**
ii) Transport layer security (TLS) **(1 mark)**
iii) IP security(IPSec) **(1 mark)**

d) Identify the four phases of a TLS handshake. **(4 marks)**

e) Briefly describe four benefits of IPSec. **(4 marks)**

Q3. a) Any human physiological or behavioral characteristics can be used as a biometric as long as it satisfies four basic requirements. Briefly describe these four requirements. **(4 marks)**

b) Briefly explain any four limitations of reusable passwords. **(3 marks)**

c) Consider a qualitative risk analysis for a business. A particular risk is expected to result in a security incident every two months at a cost of Kshs. 3000 per incidence.

i) What is the Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE) for this risk ? **(4 marks)**

ii) Suppose that the business decides not to put controls in place. Name two alternative ways that the business can treat this risk. **(2 marks)**

d) As part of the business continuity planning, a company is considering options for alternative sites for relocating the business in case of disaster. Briefly explain the concepts of Hot Site, Warm Site and Cold Site and specify in each of the three cases how long it typically would take to be operable for running functions. **(6 marks)**

Q4. 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 **(2 marks)**

b) What is the aim of using security labels ? **(1 mark)**

c) Briefly describe the following attacks and how each can be prevented.

i) Buffer overflow **(3 marks)**
ii) SQL injection **(3 marks)**
iii) Cross-Site Scripting **(3 marks)**

d) Distinguish between the following terms:

i) Encoding and encryption **(2 marks)**
ii) Symmetric and asymmetric cipher **(2 marks)**

Q5. 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)

END