THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

P.O. Box 62157
00200 Nairobi - KENYA
Telephone: 891601-6
Ext 1022/23/25

MAIN EXAMINATION

SEPTEMBER –DECEMBER 2021

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

REGULAR PROGRAMME

CMT 405: INFORMATION SYSTEMS SECURITY

Date: DECEMBER 2021	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any TWO Questions	

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

i) Cryptography **(1 mark)**
ii) Public Key Infrastructure **(1 mark)**
iii) Biometrics **(1 mark)**
iv) Business Continuity Plan **(1 mark)**

b) Give four reasons why it is impossible to simply solve all information security problems once and for all. **(4 marks)**

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

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

i) Knowledge based **(3 marks)**
ii) Object based **(3 marks)**
iii) ID based **(3 marks)**
iv) Location based **(3 marks)**

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

f) Briefly distinguish between a passive and an active attack. **(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 ? **(4 marks**

ii) If Alice receives the value 28 from Bob, what is the value of the shared secret key ? **(4 marks)**

b) Briefly describe the following three critical characteristics of information

i) Confidentiality **(1 mark)**

ii) Integrity **(1 mark)**

iii) Availability **(1 mark)**

c) Besides the three critical characteristics of information in part (b) above, briefly define which other three additional security features can be applied to enhance information security. **(6 marks)**

c) List the three main approaches to access control. **(3 marks)**

Q3. a) i)Any human physiological or behavioral characteristics can be used as a biometric as long as it satisfies four basic requirements. State and briefly describe these four requirements. **(8 marks)**

ii) A basic biometric system consists of four modules. List them. **(2 marks)**

iii) Distinguish between a stable and alterable biometric types. **(2 marks)**

b) i) Briefly describe four problems associated with reusable passwords. **(4 marks)**

ii) List four possible solutions to the problems associated with using passwords in the clear. **(4 marks)**

Q4.a) 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) List the four risk control strategies **(4 marks)**

b) 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)**

c) Briefly describe the following three information security concepts associated with risk management and give an example of each of them.

i) Vulnerability **(2 marks)**

ii) Threat **(2 marks)**

iii) Attack **(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) Distinguish between the following terms:

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

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

d) i) List four problems associated with intrusion detection systems. **(4 marks)**

ii) Detection methods used by Intrusion Detection Systems (IDS) are normally considered to be either misuse or anomaly-based. Briefly describe each of these detection methods. **(2 marks)**

e) You have been hired to assess the security weaknesses of a website managed by a local financial firm. You find that authorized user accounts are changing parameter values to directly refer to objects that these users are not authorized to access. Which type of attack does this scenario represent? **(2 marks)**

f) You click on a link in a web browser to update your contact information on a website. Your web browser is redirected to a different website that appears to look the same as the one you were on. Which type of vulnerability causes this issue? **(2 marks)**

END