(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2020/2021 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY EXAMINATIONS
YEAR THREE SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
(COMPUTER SCIENCE)

COURSE CODE: CSC 374E

COURSE TITLE: APPLIED CRYPTOGRAPHY

DATE: 20/01/2022 **TIME:** 11.00 A.M – 01.00 P.M

INSTRUCTIONS TO CANDIDATES

ANSWER **QUESTION ONE** AND **ANY OTHER TWO QUESTIONS**

QUESTION ONE (COMPULSORY) [30 MARKS]

a. List any **five** reasons why people will violate policy. **[5 marks]**

b. A firm security implementation plan can be launched and established using a series of best practices. State any **five** of these best practices. **[5 marks]**

c. Discuss briefly the benefits and limitations of asymmetric key encryption. **[6 marks]**

d. Discuss the following:
   i. Mandatory Access Control (MAC) **[2 marks]**
   ii. Discretionary Access Control (DAC) **[2 marks]**

e. Discuss the two types of errors that occur when biometrics are used for authentication. **[4 marks]**

f. Networks are subject to a number of different attacks that jeopardize their ability to support confidentiality, integrity, and availability. Describe the following network attacks:
   i. Denial of Service (DoS) **[2 marks]**
   ii. Spam **[2 marks]**
   iii. Malicious code **[2 marks]**

QUESTION TWO [20 MARKS]

a. Describe briefly the following cryptographic algorithms:
   i. RC5 **[3 marks]**
   ii. Blowfish **[3 marks]**

b. Discuss any **five** ways in which cryptographic algorithms are compromised. **[5 marks]**

c. Discuss the hash function and its role in information security. **[6 marks]**

d. State any three characteristics of a good cryptographic algorithm. **[3 marks]**

QUESTION THREE [20 MARKS]

a. One of the simplest ways to prevent attackers compromising the network is to customize the settings of the network. Customization of the network settings will give the network administrators an efficient means of monitoring network traffic. They can also put restrictions on the data, and the information exchanged over the network, to prevent exposure of the company's network, thus preventing unknown, and unauthenticated, users from accessing the network. In this regard, describe the following components of network security:
   i. Firewall **[2 marks]**
   ii. Honeypot **[2 marks]**
   iii. Intrusion Detection System (IDS) **[2 marks]**

b. (i) What benefits does the security principle known as job rotation provide? **[2 marks]**
   (ii) How is a sensitivity profiling developed and what is the benefit? **[3 marks]**

c. Describe the following methods that are used to detect an intrusion:
   i. Signature recognition. **[3 marks]**
   ii. Anomaly detection **[3 marks]**

d. Describe the following as used in access control:
   i. Authentication. **[1 mark]**
   ii. Authorization. **[1 mark]**
   iii. Auditing. **[1 mark]**

QUESTION FOUR [20 MARKS]

a. Even when everyone acknowledges that a computer crime has been committed, computer crime is hard to prosecute. State four reasons why it is hard to prosecute computer crimes. **[4 marks]**

b. Outline four categories of computer fraud. **[4 marks]**

c. Outline briefly any **four** important factors to consider when choosing a firewall solution. **[4 marks]**

d. Explain briefly the following data access principles:

i. Least privilege **[2 marks]**

ii. Separation of Duties (SoD) **[2 marks]**

e. With the aid of examples, briefly explain the following types of access control:

i. Compensation access control **[2 marks]**

ii. Directive access control **[2 marks]**

QUESTION FIVE [20 MARKS]

a. A Business Continuity Plan (BCP) should address various types of disruptive events that can target the continuity of daily business operations. Discuss. **[6 marks]**

b. Discuss briefly any five factors can increase or decrease the level of impact a threat may have on an enterprise and its assets. **[5 marks]**

c. Describe how public key encryption is used to establish the authenticity of a message that is exchanged between two parties, say Alice and Bob. **[5 marks]**

d. Describe the following general security policies that an organization may invoke:

i. Statement of authority and scope **[1 mark]**

ii. Acceptable use policy (AUP) **[1 mark]**

iii. Identification and authentication policy **[1 mark]**

iv. Internet access policy **[1 mark]**