(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
SPECIAL/SUPPLEMENTARY
2019/2020 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER EXAMINATIONS
FOR THE DEGREE
OF
BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COURSE CODE: **CSC374E**

COURSE TITLE: **APPLIED CRYPTOGRAPHY**

DATE: 08/02/2021 **TIME: 8:00 AM-10:00 AM**

INSTRUCTIONS TO CANDIDATES

Answer ALL questions ONE and ANY TWO questions

DURATION: 2Hours

KIBU observes ZERO tolerance to examination cheating

QUESTION FOUR (20 MARKS)

a. Discuss any **three** major reasons why cyber security is considered a "hard, multifaceted problem". **[6 marks]**

b. The Information Security Officer (ISO) is charged with providing support for expected governance activities. To support the governance responsibilities of the Board, the ISO is required to perform many different functions and assume numerous roles in the organization. Describe any six of these functions. **[6 marks]**

c. Audit logs can be generated at the system level to record a number of activities. State any eight activities that are recorded by audit logs. **[4 marks]**

d. 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]**

QUESTION FIVE (20 MARKS)

a. Discuss briefly any four factors can increase or decrease the level of impact a threat may have on an enterprise and its assets. **[4 marks]**

b. State any four reasons why physical security is needed. **[4 marks]**

c. Describe briefly any five IDS categories. **[5 marks]**

d. Define the following terminologies:

i. Penetration testing **[1 mark]**

ii. Recovery Point Objective (RPO) **[1 mark]**

iii. Recovery Time Objective (RTO) **[1 mark]**

iv. Business Continuity Plan (BCP) **[1 mark]**

v. Business Impact Analysis (BIA) **[1 mark]**

e. Describe the Biba security model. **[2 marks]**

QUESTION ONE (COMPULSORY) (30 MARKS)

a) Define the following terminologies:
   i. Social engineering **[1 mark]**
   ii. Virus **[1 mark]**
   iii. Logic Bomb **[1 mark]**
   iv. Sheep dip computer **[1 mark]**
   v. Keylogger **[1 mark]**

b) Access controls are necessary to protect the *confidentiality*, *integrity*, and *availability* of objects (and by extension, their information and data). In this regard describe the following types of access control.
   i. Preventive access control **[2 marks]**
   ii. Corrective access controls **[2 marks]**
   iii. Compensation access control **[2 Marks]**

c) Discuss how hashing is used in password protection. **[4 marks]**

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

e) Describe how secret key encryption is used in protecting pay TV transmissions. **[6 marks]**

f) Outline briefly any five important factors to consider when choosing a firewall solution. **[5 marks]**

QUESTION TWO (20 MARKS)

a) There are two ways to encrypt a hard drive: at the file level and at the driver level. Discuss. **[5 marks]**

b) There are many different factors that should be considered when managing cryptographic keys. Explain any four of these factors. **[4 marks]**

c) Discuss the security of public key algorithms **[7 marks]**

d) State any four weaknesses that compromise cryptographic algorithms. **[4 marks]**

QUESTION THREE (20 MARKS)

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

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

c. Explain briefly the following data access principles:
   i. Least privilege **[2 marks]**
   ii. Separation of Duties (SoD) **[2 marks]**

d. Describe the following general security policies that an organization may invoke:
   i. Statement of authority and scope **[2 mark]**
   ii. Acceptable use policy (AUP) **[2 mark]**
   iii. Identification and authentication policy **[2 mark]**
   iv. Internet access policy **[2 mark]**