(Knowledge for development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS

2017/2018 ACADEMIC YEAR

SUPPLEMENTARY/SPECIAL EXAMINATIONS

YEAR FOUR SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF

BACHELOR OF SCIENCE

(INFORMATION TECHNOLOGY)

COURSE CODE : BIT 411

COURSE TITLE : INFORMATION ASSURANCE AND SECURITY

DATE: 02/10/2018 **TIME: 11.30A.M – 1.30P.M**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTION ONE AND ANY OTHER TWO.

QUESTION ONE (30 MARKS)

a). An affine cipher with modulus 26 encrypts 4 as 2 and 7 as 17. Determine the key. [3 marks]

b). One of the main goals in an investigation is to attribute the crime to its perpetrator by uncovering compelling links between the offender, victim, and crime scene. In the context of crime scene investigation, briefly explain the two general categories of evidence produced by the Locard's Exchange Principle. Which one is more effective and why? [4 marks]

c). What is Perfect Secrecy? Describe a system that achieves it. [5 marks]

d). Explain the role of the logic of authentication. [4 marks]

e). Discuss FOUR techniques for building a reasonably safe community for electronic contact that may serve as virus prevention methods. [8 marks]

f). Justify the need of using personal firewalls to implement security in networks. [6 marks]

SECTION B

QUESTION TWO (20 MARKS)

a). Give the typical requirements of a secure distributed system. [3 marks]

b). Describe the meaning of a system in the context of security engineering. [6 marks]

c). In security engineering define what is meant by a principal and explain the meaning of identity. [5 marks]

d). Explain why challenge response identification systems are used. [2 marks]

e). Explain how public key cryptography may be used for identification. [4 marks]

QUESTION THREE (20 MARKS)

a). Explain how Denial of Service (DOS) attack constitute security threat to an information system. Cite one example. [3 marks]

b). Discuss differences between conventional and digital signatures based on the following aspects.

i. Inclusion
ii. Verification method
iii. Relationship
iv. Duplicity

[8 marks]

c). Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function. [6 marks]

d). What is a honey pot? Give TWO reasons why it may be set up. [3 marks]

QUESTION FOUR (20 MARKS)

a). Individuals and organizations need to pay attention to computer forensics. Justify this statement. [10 marks]

b).Distinguish between misuse detection and anomaly detection as forms of analysis methods giving one advantage for each. [4 marks]

c). Explain how copyrights, patents, and trade secrets are used as legal devices to protect computers, programs and data. Cite an example in each case. [6 marks]

QUESTION FIVE (20 MARKS)

a). Explain the concept of virus signatures. [4 marks]

b). Once the risk to computer security has been identified and assessed, managing the risk can be done four different ways. Elaborate these ways. [8 marks]

c). Discuss four considerations of a trusted OS during its' design. [8 marks]