03

(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2019/2020 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY EXAMINATIONS
YEAR FOUR SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF BACHELOR OF SCIENCE (COMPUTER SCIENCE)

COURSE CODE : CSC 477E

COURSE TITLE : NETWORK SECURITY

DATE: 15/02/2021 **TIME: 02:00 P.M -04:00 P.M**

INSTRUCTIONS TO CANDIDATES

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

QUESTION ONE [COMPULSORY] [30 MARKS]

a) Briefly describe the processes of encryption and decryption in relation to cryptography.

(5 marks)

b) What is the difference between Symmetric and Asymmetric key encryption? (4 marks)

c) James and Alexander are having a debate about Public Key Infrastructure (PKI). James says that it is simply a way of authenticating users. However, Alexander argues that it is a type of encryption algorithm. They have asked you to decide who is correct.

i. Briefly outline the purpose of PKI. You should also explain what is meant by a certificate authority and digital certificate. (6 marks)

ii. Are James's and Alexander's opinions about Public Key Infrastructure correct or incorrect? For each opinion, you should provide ONE (1) reason for why it is either correct or incorrect

(4 marks)

d) Briefly explain what is by an Authentication Header (AH) and an Encapsulating Security Payload (ESP). (6 marks)

e) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. (5 marks)

QUESTION [20 MARKS]

a) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these FIVE (5) requirements. (5 marks)

b) There are several methods of achieving secure remote access. One important method is to use a VPN. Explain if/ how a VPN achieves each of the requirements in part (a) (5 marks)

c) Draw a diagram to show where IPSec fits in the TCP/IP model. (10 marks)

QUESTION [20 MARKS]

a) Explain what is meant by a digital signature and describe how it is generated (6 marks)

b) Does a digital signature ensure the entire message is encrypted? You should provide ONE (1) reason to support your answer. (3 marks)

c) Explain what is meant by the term firewall in network security and discuss how it is used in network architectures. (7 marks)

d) Firewalls use Access Control Lists (ACL). Explain what is meant by an ACL and typical contents. (4 marks)

QUESTION [20 MARKS]

a) Confidentiality, Integrity and Availability are core attributes in security. Identify THREE (3) threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. (6 marks)

b) Discuss TWO (2) alternative methods of authentication and outline ONE (1) advantage or disadvantage of each method. (4 marks)

c) James and Alexander are having another debate about computer and network security. James says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with James? You should explain your answer with TEN (10) reasons. (10 marks)

Question [20 MARKS]

a) Briefly describe the term vulnerability in the context of network security and provide THREE (3) examples of vulnerabilities in a network. (6 marks)

b) Explain what is meant by a vulnerability assessment in the context of network security and provide THREE (3) reasons why it is important. (6 marks)

c) Confidentiality, Integrity and Availability are core attributes in security. Identify FOUR (4) threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. (8 marks)