(Knowledge for Development)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2019/2020 ACADEMIC YEAR

SPECIAL /SUPPLEMENTARY EXAMINATIONS
YEAR FOUR SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
BACHELOR OF COMPUTER SCIENCE

COURSE CODE : CSC 321

COURSE TITLE : COMPUTER SYSTEM SECURITY

DATE: 12/02/2021 TIME: 08.00 A.M – 10.00 A.M

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a) Define the following terms as used in computer security.

i. A logic bomb **[1 mark]**

ii. Trap Door **[1 mark]**

iii. Man in the Middle Attack **[1 mark]**

iv. Replay Attack **[1 mark]**

b) Differentiate between the following terminologies.

i. Cryptanalysis and cryptography **[2 marks]**

ii. Symmetric key and Asymmetric key encryption **[2 marks]**

iii. Public algorithms and proprietary algorithms **[2 marks]**

c) Discuss the various components of a basic cryptosystem **[6 marks]**

d) Describe FOUR main security requirements that cryptography addresses. **[4 marks]**

e) Evaluate the differences between passive and active attacks in computer security. **[6 marks]**

f) Why does Moore's Law make it increasingly more important to create strong passwords? **[4 marks]**

QUESTION TWO [20 MARKS]

a) What is Pretty Good Privacy (PGP)? **[2 marks]**

b) Describe how Kerberos implements authentication and confidentiality. **[4 marks]**

c) Discuss the working of S/MIME in the provision of security services. **[6 marks]**

d) Cyber warfare between nations is on the rise. What could you do to minimize corporate risk if you were the CEO of a company? **[4 marks]**

e) What is IP Spoofing? What implications does it have on network security? **[4 marks]**

QUESTION THREE [20 MARKS]

a) Identify the six secret values are then derived from master secret of SSL session keys. **[6 marks]**

b) Differentiate between TLS and SSLv3 protocols. **[8 marks]**

c) Analyze the benefits and limitations of employing communication security at transport layer. **[6 marks]**

QUESTION FOUR [20 MARKS]

a) Differentiate between Message and Entity authentication. **[2 marks]**

b) Identify the cryptography primitives that can be selectively used to provide a set of desired security services. **[4 marks]**

c) Cryptographic primitives are intricately related and they are often combined to achieve a set of desired security services from a cryptosystem. Using a comparative analysis, explain how the primitives in (b) above may or may not affect confidentiality, integrity, authentication, and non-repudiation. **[8 marks]**

d) Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. Discuss the salient features of this encryption scheme. **[6 marks]**

QUESTION FIVE [20 MARKS]

a) Why is it that a chosen plaintext attack cannot be used to break a one-time-pad? **[7 marks]**

b) If it takes one day to break a 32-bit symmetric cipher key by trying all possible decryption cipher keys, how long will it take to break a 128-bit cipher key? **[8 marks]**

c) What data can be hashed using SHA1 that result in a string in it of the first three letters of your name? **[5 marks]**