105

(University of Choice)

MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY (MMUST)

UNIVERSITY EXAMINATIONS

2022/2023 ACADEMIC YEAR

THIRD YEAR FIRST SEMESTER EXAMINATIONS

FOR THE DEGREE

OF

BACHELOR OF SCIENCE INFORMATION & KNOWLEDGE MANAGEMENT

COURSE CODE: BIT 315

COURSE TITLE: INFORMATION ASSUARANCE & SECURITY

DATE: 14/12/2022 **TIME:** . 8:00-10:00AM

INSTRUCTIONS TO CANDIDATES

Question ONE (1) in Section A is compulsory
Answer any other 2 questions from Section B

TIME: 2 Hours

MMUST observes ZERO tolerance to examination cheating

Question One

a) Explain the key requirements of a secure distributed system. (6 marks)
b) Describe an information system in the context of security engineering. (6 marks)
c) Explain what is meant by a social engineering attack on a password. (4 marks)
cd) Explain how a man-in-the-middle attack on a Wireless network can be defeated.(4 marks)
e) In general, there are three types of identity authentication tasks. Explain these tasks.(4 marks)
f) Using illustrations describe the terms Honeypot, Honeynet and Padded Cell Systems when used in relation to information security and describe how each can be used to protect and secure an organisation's information assets (9 marks)

Question Two

a) Using examples explain the role of the logic of authentication. (5 marks)

b) An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks. (10 marks)
c) Discuss the three main concerns with the use of passwords for authentication. (5 marks)

Question Three

a) Describe the goals an ideal password authentication scheme should achieve. (10 marks)

b) Explain how access control lists are use to represent access control matrices. (4 marks)

c) Describe the environments in which access control matrices are widely used and their advantages and disadvantages.. (6 marks)

Question Four

a) Explain how capability lists are used to represent access control matrices. (6 marks)
b) How might a hacker attempt to attack a cryptosystem and how can an organisation best defend itself against such an attack? (6 marks)
c) Discuss the main problem associated with the use of capability lists and its consequences (4 marks)
d). Explain how public key cryptography may be used for identification. (4 marks)

Question Five

a) Joseph proposed two measures of security: unicity distance and cover time. Explain how each of these concepts seeks to provide an indication of the security of a cipher system and outline the theoretical concept which has now superseded the notion of cover time. (10 marks)

b) You are finalizing your security test status report for a project that is ready for deployment into production. There is a high degree of risk for this project due to the nature of the system. As a result, you want to place particular emphasis on risk. Based on this, what is the best way to articulate risk on your report? (6 marks)

c) The concept of computational complexity has superseded the notion of covertime as a measure of the security of a cryptosystem. Explain how computational complexity theory provides the theoretical basis for the design of modern scalable cryptosystems. (4 Marks)