



MACHAKOS UNIVERSITY

University Examinations for 2022/2023 Academic Year

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY

SECOND YEAR SECOND SEMESTER EXAMINATION FOR

BACHELOR OF SCIENCE (CLOUD COMPUTING AND SECURITY)

SCC230: NETWORK SECURITY CONCEPTS

DATE: 18/4/2023

TIME: 2:00 – 4:00 PM

Instruction: Answer Question ONE and any other TWO Questions

QUESTION ONE (COMPULSORY) (30 MARKS)

- a) Highlight **two** reasons for securing information systems. (2 marks)
- b) Discuss **four** categories of computer security threats (8 marks)
- c) Using a well labeled diagram, illustrate the CIA security triad (4 marks)
- d) Differentiate the following terms as used in information security
 - i) Interruption and interception (2 marks)
 - ii) Network and Internet security (2 marks)
 - iii) Peer entity and data origin authentication (2 marks)
- e) You have been hired as a network security officer in a newly established software company. As part of your mandate you are to come up with measures to secure data in the company as well as ensure that the products released to the market are secure. Analyze **four** security mechanisms you would put in place to achieve that. (8 marks)
- f) Highlight **two** encryption techniques. (2marks)

QUESTION TWO (20 MARKS)

- a) Using a well labeled diagram, demonstrate how S-DES data encryption is achieved. (8 marks)
- b) Fanaka Bank is a large bank with hundreds of branches that are connected to a central server computer system. Some branches are connected over dedicated circuits and others use multiprotocol label switching (MPLS). Each branch has a variety of client computers and ATMs connected to a server. The server stores the branches and transmits it several times during the day to the central computer system. Tellers at each branch site use a four-digit numeric password, and each teller's computer is transaction-coded to accept only its authorized transactions.
- i) Perform a security risk assessment. (6 marks)
- ii) Compile a list of hardware and software that this bank should have used for each client connectivity with the server. (6 marks)

QUESTION THREE (20 MARKS)

- a) Discuss the similarities and differences between symmetric and asymmetric encryption. (4 marks)
- b) Demonstrate how the following security mechanisms are implemented.
- i). Kerberos (5 marks)
- ii). Secure Hash Algorithm (SHA-1) (5 marks)
- c) Biometric technology has been available for a number of years. However, its adoption has been slow.
- i). Discuss **three** factors inhibiting the adoption (3 marks)
- ii). Propose measures which may increase this adoption for each factor in (i) above (3 marks)

QUESTION FOUR (20 MARKS)

- a) Demonstrate **four** ingredients of data encryption. (8 marks)
- b) Analyze **four** security mechanisms applied in a high risk environment. (8 marks)
- c) Differentiate between active and passive attack. (4 marks)

QUESTION FIVE (20 MARKS)

- a) Briefly explain the following terms, citing an example of a technique used to implement it:
- (i) secure commitment; (2 marks)
 - (ii) mandatory access control policy; (2 marks)
 - (iii) perfect secrecy; (2 marks)
 - (iv) message authentication code. (2 marks)
- b) Discuss the **three** terms; Caesar, mono alphabetic and play fair cyphers as used in data encryption (6 marks)
- c) Describe **three** steganographic techniques which have been used historically to secure information. (6 marks)