



MACHAKOS UNIVERSITY

University Examinations for 2021/2022

SCHOOL OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY
SECOND YEAR SPECIAL / SUPPLEMENTARY EXAMINATIONS FOR
BACHELOR OF SCIENCE (COMPUTER SCIENCE)
BACHELOR OF SCIENCE (INFORMATION TECHNOLOGY)
SIT 230/SCO406: COMP AND INFORMATION SECURITY

DATE: 29/8/2022

TIME: 2.00-4.00 PM

INSTRUCTIONS:

Answer Question ONE and other TWO Questions

QUESTION ONE (COMPULSORY)

- a) Differentiate the following terms as used in information security
- i. Risk and threat (2 marks)
 - ii. Passive and active attack. (2 marks)
 - iii. Identification and authentication (2 marks)
 - iv. . Data Modification and Fabrication (2 marks)
- b) Highlight three computer information security goals. (3 marks)
- c) Highlight three reasons for securing information systems. (3 marks)
- d) Analyze the CIA security triad (6 marks)
- e) Assume you have been hired as a security consultant by Kenya Revenue Authority, after several cases of security compromise. Discuss five tools you would employ to mitigate the risks and how you would evaluate their effectiveness. (10 marks)

QUESTION TWO (20 MARKS)

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

QUESTION THREE (20 MARKS)

- a) Differentiate between Caesar, mono alphabetic and play fair cyphers. (6 marks)
- b) When two parties are communicating over a secure network, data is usually encrypted. Demonstrate how the encryption happens and the mechanisms involved in facilitating access to the information on both ends. (8 marks)
- c) Discuss three steganography techniques which have been used historically to secure information. (6 marks)

QUESTION FOUR (20 MARKS)

- a) 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 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 FIVE (20 MARKS)

- a) Discuss five security services. (10 marks)
- b) Analyze five security mechanisms applied in a high risk environment. (10 marks)