



MACHAKOS UNIVERSITY

University Examinations for 2018/2019

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY

FOURTH YEAR SECOND SEMESTER EXAMINATION FOR

BACHELOR OF SCIENCE (MATHEMATICS AND COMPUTER SCIENCE)

SCO 406: COMPUTER SYSTEM SECURITY

DATE: 9/5/2019

TIME: 2.00-4.00 PM

INSTRUCTIONS

Answer **question ONE** and any other **TWO** questions.

QUESTION ONE (30 MARKS)

- a) Differentiate between stenography and cryptography. (2 marks)
- b) 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)
- c) List three types of threats to computer systems. (4 marks)
- d) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. (3 marks)
- e) Explain what is meant by a digital signature and describe how it is generated. (3 marks)
- f) Given a communication that applies secret key cryptography among five individuals, calculate the number of keys used. (3 marks)
- g) Describe THREE main attack techniques to operating system. (3 marks)
- h) Name TWO main categories of constraints in database management and explain why each category is important. (4 marks)
- i) List and explain THREE different types of firewalls. (3 marks)

QUESTION TWO (20 MARKS)

- a) Explain how public key cryptography may be used for identification. (4 marks)
- b) Describe in details the THREE types of information that can be used in authentication (6 marks)
- c) Using a well labeled diagram, show the operation of data encryption standard (DES) (10 marks)

QUESTION THREE (20 MARKS)

- a) Briefly explain how RSA algorithm works. (Use a suitable example). (7 marks)
- b) Explain the concept and importance of confusion, diffusion. (4 marks)
- c) Discuss the concept of intrusion prevention and detection. (4 marks)
- d) Using suitable example how does access control list (ACL) work. (5 marks)

QUESTION FOUR (20 MARKS)

- a) Using Diffie Hellman algorithm and supposing Alice and Bob agrees that N is 11 and α is 2. Alice decides to choose X_A as 9 and Bob chooses X_B as 3. Compute Y_A and Y_B . What is the key? (10 marks)
- b) Using Playfair matrix encrypt this message: I Must see you over Cadogan West. Coming at once. Use "University" as the key word (10 marks)

QUESTION FIVE (20 MARKS)

- a) Describe the risk management process in details. (10 marks)
- b) On computer system, the most common form of authentication is the use of username and password. While these two have served their purpose, they are no longer adequate today. Highlight and explain FIVE reasons why this is the case. (10 marks)