



MACHAKOS UNIVERSITY

University Examinations for 2017/2018

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY

**FOURTH YEAR SECOND SEMESTER EXAMINATION FOR BACHELOR OF
SCENCE (MATHEMATICS AND COMPUTER SCIENCE)**

SCO 406: COMPUTER SYTEMS SECURITY

DATE: 20/12/2017

TIME: 11.00-1.00 PM

INSTRUCTIONS

Answer Question ONE and any other TWO Questions

QUESTION ONE (30 MARKS)

- a) Differentiate between stenography and cryptography. (2 marks)
- b) Describe five main objectives of information system security. (5 marks)
- c) List three threats that result from cybercrimes. (3 marks)
- d) What is residue risk? (2 marks)
- e) Give three main techniques for mitigating risks in a computerized environment. (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. (6 marks)
- i) Give three main 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) Explain briefly the concepts of one-way function, one-way hash function and trapdoor one way function. (5 marks)
- b) Explain how an RSA key is created. (10 marks)
- c) List at least FIVE kind of information contained in a certificate. (5 marks)

QUESTION FOUR (20 MARKS)

- a) Using Diffie Hellman algorithm and supposing Alice and Bob agrees that N is 7 and α is 3. Alice decides to choose X_A as 2 and Bob chooses X_B as 3. What is Y_A and Y_B ? Calculate the key. (10 marks)
- b) Clearly describe secure electronic transactions (SETs). (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 a username and a password. While these two have served their purpose, they are no longer adequate in today world. Highlight and explain FIVE reasons why this is the case. (10 marks)