MACHAKOS UNIVERSITY

University Examinations for 2018/2019

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY

THIRD YEAR SPECIAL/SUPPLEMENTARY EXAMINATION FOR

BACHELOR OF SCIENCE (INFORMATION TECHNOLOGY)

SIT 302: INFORMATION SYSTEMS SECURITY

DATE: **TIME:**

INSTRUCTIONS: Answer Question One and Any Other Two Questions

QUESTION ONE (30 MARKS)

a) Distinguish between the following terms, giving examples of each;

i. Computer security and Information security (5 marks)

ii. Authorization and cryptography (5 marks)

b) A computer virus is a self propagating computer program designed to alter or destroy a computer system resource. Describe three techniques that can be used to manage viruses in a computer. (6 marks)

c) Differentiate between public and private keys as used in cryptography. (4 marks)

d) A firewall is hardware, software or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network. Discuss five limitations of firewalls (10 marks)

QUESTION TWO (20 MARKS)

a) Software access control falls into two types; point of access and remote monitoring. Explain five techniques that can be used to implement access control in a typical computing system. (10 marks)

b) Cryptography has become the main tool for providing the needed digital security in the modern digital communication medium that far exceeds the kind of security that was offered by any medium before it. Describe five basic components of cryptography (10 marks)

QUESTION THREE (20 MARKS)

a) Rapid advances in technology have resulted in efficient access control tools that are open and flexible, while at the same time ensuring reasonable precautions against risks. By use of clear illustrations differentiate between access terminal and video surveillance as access control tools. (8 marks)

b) RSA can be used to support secrecy, authenticity and integrity. Illustrate how it can be used in the following scenarios;

i) Mary wishes to send a secret message M to John (3 marks)

ii) Mary wishes to send a message M to John such that John is assured that the message could only have originated from Mary. (3 marks)

iii) Mary wishes to send a secret message M to John such that John is assured that the message could only have originated from Mary and that the message was not modified during its transit from Mary to John (6 marks)

QUESTION FOUR (20 MARKS)

a) Describe the message authentication process using;

i. Symmetric encryption (3 marks)

ii. Hash function (3 marks)

b) Security of the operating system is very important as far as the overall system security is concerned. Discuss five security features of an ordinary operating system. (10 marks)

c) The security policy of an organization is built in stages and each stage adds value to the overall product. Highlight four vulnerabilities that a security policy may cover. (4 marks)

QUESTION FIVE (20 MARKS)

a) KCB has successfully implemented IS security on their distributed systems especially in system access control.

i. Discuss three techniques that they might have used to secure their network. (6 marks)

ii. Explain three main objectives of IS security that they wanted to achieve. (6 marks)

b) Explain three methods that can be used to ensure security of electronic payments. (6 marks)

c) Define computer forensics. (2 marks)