KENYATTA UNIVERSITY

UNIVERSITY EXAMINATIONS 2011/2012

SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

SIT 302: INFORMATION SYSTEM SECURITY EXAMINATION

DATE: Tuesday 3rd April 2012 TIME 2.00 PM –4.00PM

INSTRUCTIONS: ANSWER QUESTION ONE AND ANY OTHER TWO QUESTIONS

QUESTION ONE Total 30 marks

a) Explain the meaning of the term information security (3 marks)

b) A need exists for information security concerns. Explain any TWO contributing factors for this concern (2 marks)

c) Differentiate between information security, computer security and information assurance (6 marks)

d) Explain the differences between Virus, Worm and Trojan horse (6 marks)

e) What are the differences between Plain text and Ciphertext (4 marks)

f) Describe what the cookies are, and explain how they can be an information security threat (5 marks)

g) Explain the main differences between a firewall and a proxy server (4 marks)

QUESTION TWO Total 20 marks

a) Explain the meaning of the following information security terms:

i. Confidentiality (3 marks)

ii. Integrity (3 marks)

iii. Availability (3 marks)

iv. Non-repudiation (3 marks)

v. Authentication (3 marks)

b) A hash functions, also known as message digests or one-way encryption is an important security feature in information security configuration. Explain how a hash function is used to provide information security (5 marks)

QUESTION THREE Total 20 marks

a) Assume that you are training users in your organization on their roles to ensure that information in your organization is secure, list **FOUR** roles you would consider necessary for the users to adhere to. (8 marks)
b) List **FOUR** information security guidelines/tips that you would give these users in order to enforce the roles in (a) above (8 marks)
c) What are the differences between digital certificate encryption and the traditional encryption? (4 marks)

QUESTION FOUR Total 20 marks

a) Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are two authentication methods. Explain how authentication is achieved using these methods. (6 marks)
b) Using a well-labeled diagram, explain how three types of cryptography: secret-key, public key, and hash function are used for encryption and decryption of information in a network. (9 marks)
c) Define the term 'information security model'. (2 marks)
d) List any **THREE** characteristics than an information security model should have. (3 marks)

QUESTION FIVE

a) Explain how data encryption is achieved using the following encryption methods;
    i. Mono-alphabetic system (3 marks)
    ii. Poly-alphabetic system (3 marks)
    iii. Caesar cipher (4 marks)
b) List and discuss **FIVE** design considerations that should be adhered to while designing an information security system. (10 marks)

****