KENYA METHODIST UNIVERSITY

END OF 1ST TRIMESTER 2010 EXAMINATIONS

FACULTY	**:**	**COMPUTING AND INFORMATICS**
DEPARTMENT	**:**	**COMPUTER INFORMATION SYSTEMS**
UNIT CODE	**:**	**CISY 431**
UNIT TITLE	**:**	**INFORMATION SYSTEMS SECURITY**
TIME	**:**	**2 HOURS**

Instructions:

- *Answer question 1 and any other 2 questions.*

Question 1 (30 marks)

a) Define the following information security terms; (5 mks)

i) Exposure

ii) Threats

iii) Vulnerability

iv) Attack

v) Security control

b) Differentiate passive attacks from active attacks. (4 mks)

c) Describe the following broad internet connection policies. (4 mks)

i) Paranoid

ii) Promiscuous

iii) Permissive

iv) Prudent

d) Explain using examples the following classical cipher techniques. (6 mks)

i) Mono alphabetic substitution ciphers

ii) Poly alphabetic substitution ciphers

iii) Transposition ciphers

e) Differentiate a security plan from a security policy. (4 mks)

f) The following is an example of a security usage policy statement (except) state seven specific security attributes that the below policy statement addresses and suggest the possible solution for each. (7 mks)

Access to the internet based KeMU web server resources shall only be allowed for express purpose of performing work related duties. This policy is to ensure the effective use of networking resources and shall apply equally to all employees and students. This policy shall be enforced during both production and non-production time periods. All web server access will be monitored by ICT personnel.

Employees and students may be required to justify web server access to their immediate supervisor. Failure to comply with this policy will result in issuance of a written warning. For information of what is considered appropriate web server access of internet resources, please consult your direct supervisor for usage instructions.

Question 2 (20 marks)

a) Discuss the following security mechanism and techniques. (6 mks)

- i) Physical
- ii) Administrative
- iii) Logical security

b) Explain the term principle of effectiveness in information system security. (2 mks)

c) State and explain three classical message concealment techniques used in cryptography. (6 mks)

d) Differentiate symmetric key cryptography from asymmetric key cryptography. (2 mks)

e) Explain the following terms as used ISS.

- a) Phishing (2 mks)
- b) Cryptoanalysis (2 mks)

Question 3 (20 marks)

a) Explain the following encryption standards

- i) DES (3 mks)
- ii) RSA (3 mks)
- iii) Rijndael (3 mks)

b) Giving an example, define programmed threats. (3 mks)

c) Explain the following types of malicious software

- i) Worms (2 mks)
- ii) Trojans (2 mks)

d) Describe certificate authority (CA) (2 mks)

e) Discuss the problem Kerberos was designed to address. (2 mks)

Question 4 (20 marks)

a) Internetwork security is both fascinating and complex. Give and explain at least four reasons for this argument. (8 mks)

b) Briefly explain Deffie-Hellman key exchange. (4 mks)

c) Define the term firewall. (2 mks)

d) Explain six firewall design goals. (6 mks)