[All Rights Reserved]

SLIATE

SRI LANKA INSTITUTE OF ADVANCED TECHNOLOGICAL EDUCATION

(Established in the Ministry of Higher Education, vide in Act No. 29 of 1995)

Higher National Diploma in Information Technology

Second Year, First Semester Examination – 2016

HNDIT 2301 - Operating Systems & Computer Security

Operating Systems & Cryptography

Instructions for Candidates:
Answer Any Four (04) Questions Only
All question carry equal marks

No. of questions : 05
No. of pages : 03
Time : **Two (02) hours**

Question: 01

(i) What is meant by computer security? (03 marks)

(ii) Briefly explain the differences between security service and security mechanism. (05 marks)

(iii) What is security attack? Briefly describe passive attack and active attack? (05 marks)

(iv) Explain the model of network security using suitable diagram. (06 marks)

(v) Describe the following security threats.

a) Interception

b) Modification

c) Interruption

(06 marks)

(Total 25 Marks)

Question: 02

(i) List out authentication methods available in database security. (03 marks)

(ii) List out four (4) responsibilities of a database administrator. (04 marks)

(iii) Briefly explain characteristics of a good password. (04 marks)

iv Briefly explain the two types of lock in database? (04 marks)

(v) Briefly explain five expected security requirements in a database. (10 marks)

(Total 25 Marks)

Question: 03

(i) Match the correct items from left column (1-9) with right column (A-I). (09 marks)

1	Decipher (decrypt)	A	The field of both cryptography and cryptanalysis
2	Cipher text	B	The coded message
3	Cryptology	C	Algorithm for transforming plaintext to cipher text
4	Key	D	The original message
5	Encipher (encrypt)	E	The study of principles/ methods of deciphering cipher text without knowing key
6	Cryptography	F	Recovering plaintext from cipher text
7	Plaintext	G	Study of encryption principles/methods
8	Cryptanalysis (codebreaking)	H	Converting plaintext to cipher text
9	Cipher	I	Information used in cipher known only to sender/receiver

(ii) Categorize cryptography into three according to the characteristics.

(03 marks)

(iii) Explain the following with suitable examples

a) Caesar cipher

b) Simple columnar transposition technique (02x04 = 08 marks)

(iv) Write algorithm (C++ / Java) to encrypt a text using Caesar cipher. (Write as much as simplest) (05 marks)

(Total 25 Marks)

Question: 04

(i) Define the following terms.

a) Digital signature

b) Digital certificate (04 marks)

(ii) Compare and contrast Digital signature and Manual signature. (03 marks)

(iii) List out three (3) possible digital certificate types. (03 marks)

(iv) What are the contents of a "Digital Certificate"? (04 marks)

(v) What is hashing in computer security? List two different hashing algorithms. (05 marks)

(vi) Suppose that one needs to prove that he/she, and not someone else, has sent a particular message to a colleague, propose a method to achieve this, by assuming that he/she is using public key encryption. (06 marks)

(Total 25 Marks)

Question: 05

(i) What is malicious software? (02 marks)

(ii) List three (3) possible counter measures on a virus attack. (03 marks)

(iii) Define the term "Trapdoor", and distinguish it from a computer virus. (04 marks)

(iv) What are the four (4) basic types of firewalls? (02 marks)

(v) Define and compare the concepts of "packet filtering" and "application level firewalls". (05 marks)

(vi) Briefly explain any three (03) of followings

a) Password Guessing

b) password capture

c) Biometric authentication

d) Approaches to Intrusion Detection

e) DOS & DDOS attacks

(09 marks)

(Total 25 Marks)