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 55

Second Year, First Semester Examination – 2019

HNDIT2301/ IT3004 Operating System and Computer Security/ Operating System and Information Security/ Operating System and Cryptography

Instructions to Candidates:
Answer four (04) questions only.
All Questions carry equal marks

No of Question: 05
No. of Pages : 02
Time: Two Hours (02)

Question 01.

(i) Describe the term Security Mechanism (04 Marks) 4
Design to detect prevent Security attack

(ii) Name one security service / mechanism for achieving the following security objectives:
a) Integrity – Digital Signatures
b) Data confidentially – Encryption (04 Marks) 4

(iii) Name five major categories of security services defined in X.800 OSI security architecture. (05 Marks) 5
Authentication Access Control Data Confidentiality Data Integrity Non Repudiation

(iv) Using a diagram briefly explain a model which is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. (06 Marks) 5

(v) Discuss the need of computer security in the present business world. (06 Marks)

(Total 25 Marks)

Question 02.

(i) Briefly explain the followings:
a) Rail Fence cipher
b) Product Ciphers (04 Marks)

(ii) Write C++ program to convert plain text into cipher text. (key is 3) (04 Marks) 4

(iii) Name five components in Symmetric Cipher Model (05 Marks)

(iv) Encrypt the message "CAESAR" using Caesar cipher algorithm defined as C=(P+3) mod 26 (06 Marks) 6

(v) Compare the followings:
a) Block Ciphers and Stream Ciphers
b) Encryption and Steganography (06 Marks) 5

(Total 25 Marks)

Question 03.

(i) Name the keys used in Public-Key Cryptography. What is the purpose of each key? (04 Marks)

(ii) Briefly explain the followings:
   a) Direct Digital Signatures
   b) Message Authentication Code (MAC)
   c) Asymmetric (Public Key) Encryption (09 Marks)

(iii) Name three basic authentication models with an example for each. (06 Marks)

(iv) Hashing is a mathematical technique used to assure message integrity. Explain how hashing helps to achieve the message integrity. (06 Marks)

(Total 25 Marks)

Question 04.

(i) A condition or restriction that is applied to a particular set of data is commonly termed as database integrity control on constrains. Name two types of constraints in SQL. (04 Marks) 4

(ii) Briefly explain the followings:
   a) Non-malicious Program Errors
   b) Features of protected OS
   c) Design principles trusted operating system design. (09 Marks) 6

(iii) Briefly explain action you can take against virus attack. (06 Marks) 6

(iv) Compare and contrast the followings:
   a) Trojan Horse and Logic Bomb
   b) Logical database integrity and Physical database integrity (06 Marks)

(Total 25 Marks)

Question 05.

(i) Name four services provided by a firewall for enabling network security. (04 Marks)

(ii) Briefly explain the followings:
   a) SSL Architecture
   b) IPsec Services
   c) Packet filtering firewall
   d) Approach to implement Information Security Policy
   e) Characteristics of a good password (15 Marks)

(iii) A security Expert states that "An Intrusion Detection System provides more effective way of handling security threats than an anti-virus software". Do you agree with this opinion? Explain your answer. (06 Marks)

(Total 25 Marks)