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 – 2015

IT3004 Operating Systems and Computer Security

HNDIT2301 Operating Systems and Cryptography

Instructions:
Answer any Four (04) questions
All Questions carry equal marks

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

Question 01

(i) List security triad. (03 marks)

(ii) Describe "Security Attack" and "Security Mechanism". (04 marks)

(iii) Five major categories of security services are defined in X.800 OSI security architecture. Briefly explain any three of them. (06 marks)

(iv) Briefly explain "Model for Network Security" using a diagram. (05 marks)

(v) Define "Information Security Policy". (03 marks)

(vi) Information Security Policy (ISP) is important to an organization. Do you agree with this statement? Justify your answer. (04 marks)

(Total 25 marks)

Question 02

(i) Define the term cryptanalysis. (03 marks)

(ii) Briefly explain the following terms. (05 marks)

a) Encryption
b) Decryption
c) Cipher
d) Plane text
e) Key

(iii) Encryption algorithms are categorized as "Substitution Ciphers" and "Transposition Ciphers". Give two examples for each. (04 marks)

(iv) Compare the characteristics of "Block Ciphers" with "Stream Ciphers". (04 marks)

(v) Encrypt the message "**easy question**" using Caesar Cipher defined as C=E(P)=(Pi+3) mod 26 (09 marks)

(Total 25 marks)

Question 03

(i) Asymmetric encryption is developed to address two key issues. Explain one of them briefly (02 marks)

(ii) Public key algorithm relies on two keys. Briefly explain two characteristics of public key algorithm. (04 marks)

(iii) Name two alternative functions used in message authentication. (04 marks)

(iv) What is a Digital Certificate? (02 marks)

(v) Explain the role of a Key Distribution Centre in a Two Key Crypto System (05 marks)

(vi) The Digital Signature is a well-known modern security mechanism that assures confidentiality, integrity and availability of information. It uses a number of security techniques in performing its task. Discuss the benefits and limitations of Digital Signature. (08 marks)

(Total 25 marks)

Question 04

(i) Malicious software is categorized in to two types. Name them and give two examples for each category. (04 marks)

(ii) State three (03) common non-malicious program errors. (03 marks)

(iii) List down three (03) authentication methods and give one example for each method (03 marks)

(iv) State the phases of virus life cycle. (04 marks)

(v) Explain methods used for buffer overflow protection. (04 marks)

(vi) Briefly explain "Procedure Based Access Control" and "Role Based Access Control" (04 marks)

(vii) State services available in Trusted Operating System. (03 marks)

(Total 25 marks)

Question 05

Write short notes on any **five (5)** of the following topics.

(i) Firewall (hint: construct your answer considering what it is, limitations and types firewalls)

(ii) Intrusion Techniques and Approaches to Intruder Detection.

(iii) Security Socket Layer Protocol

(iv) IP Security

(v) Database Integrity

(vi) Database Administrator

(vii) Database recovery

(05 * 5 marks =**25 m**