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 System and Information Security/
IT 3004 – Operating System and Computer Security/
HNDIT 2301 - Operating System and Cryptography

Instructions for Candidates:

Answer only **04 Questions**

No. of Questions: 05

No. of Pages : 03

Time: Two (02) hours

Q1 i. There are 3 basic concepts associated in information security. Those are called security triad. One of them is Confidentiality. Name the other two factors. (02 Marks)

ii. Write the definition of a Security Service given as in X.800 OSI Security Architecture (03 Marks)

iii. Some description used in Information Security are given below. Write suitable term that matches with those descriptions.

a). A week point in a system where a threat can sneak in.

b). Any procedure that is in place to assure security of a system

c). a potential damage that can be materialized through some flaw in the system. (06 Marks

iv. X.800 OSI Security Architecture categorized security mechanisms in two ways. Name two categories and give examples for each. (08 Mark

v. Assume you are the Network Administrator of your organization. You want to improve Access Security. Briefly explain how you implement it according to Model for Network Access Security. (06 Mar

(25 Mar

Q2 i. There are two requirements for secure use of symmetric encryption. Name them. (02 Marks)

ii. State three components related to Symmetric Cipher Model with a suitable diagram. (06 Marks)

iii. Cryptographic techniques can be characterized in three ways. One of them is" how the plain text is processed". Give two cryptographic algorithm types, used to process plain text, with examples for each type. (04 Marks)

iv. Briefly explain any four from the following list. (08 Marks)

a). Brute Force Search
b). Substitution Ciphers ✓
c). One-Time Pad
d). Rail Fence cipher ✓
e). Product Ciphers ✓
f). Steganography

v. Convert following word "block" into cipher text using Caesar Cipher algorithm as given below:

$C = (P + 3) \bmod (26)$ (05 Marks)

(25 Marks)

Q3 i. Name the keys used in for encryption and decryption process in Symmetric and Asymmetric Encryption. (04 Marks)

ii. Name four methods used for distribution of Public Keys. (04 Marks)

iii. Lahiru and Raj are two friends who has obtained public key algorithms from a key distribution Centre. They both have public keys known by everyone, and a private key known only by him. mention which key they can use in following situations: (08 Marks)

a). Raj wants to encrypt the message using Asymmetric Encryption and send it to Lahiru.
b). Raj wants to include digital signature for message.
c). Lahiru wants to decrypt the cipher text he received from Raj, using asymmetric encryption.
d). Lahiru wants to verify the digital signature of the message he has received from Raj.

iv. Why message authentication is important? Give three reasons. (03 Marks)

v. Compare and contrast hash function and Message Authentication Code (MAC). (06 Marks)

(25 Marks)

Q4 i. State four protection features for databases. (04 Marks)

ii. Describe "Intruder" in terms of an information system, giving three examples for different types of intruders. (06 Marks)

iii. A multi-level database is a specially designed database to enhance security of data. Give three factors that should be considered in designing multi-level databases. (03 Marks)

iv. State three implementation mechanisms for multi-level databases. (06 Marks)

v. "Program security is equally important as data and database security measures in software applications." critically discuss the above statement. (06 Marks)

(25 Marks)

Q5 Write short notes on any five topics from the following list. (05 Marks X 5)

i. Limitations of firewalls

ii. Password Security

iii. Honey Pots

iv. Stateful Inspection Firewall

v. Buffer Overflow

vi. Information Security Policy

vii. Role Based Access Control

viii. Design principles for trusted operating systems

(25 Marks)

THE END