



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 – 2017

HNDIT 2301 - Operating Systems & Computer Security

Instructions for Candidates:

No. of questions : 05

Answer Any Four (04) Questions Only

No. of pages : 02

All question carry equal marks

Time : **Two (02) hours**

Question 01

- I. Explain the term cryptosystem. (02 Marks)
- II. What do you mean by cryptanalysis? (03 Marks)
- III. List out the three (3) concepts associate in information security and indicate one security services or mechanism for each. (06 Marks)
- IV. Briefly explain the following terms.
 - a. Vulnerability
 - b. Security Control
 - c. Security Service (03x03= 09 Marks)
- V. Encrypt the message “BEST QUESTIONS” using Caesar encryption algorithm defined as $C=E(P)=(P_i+3) \text{ mod } 26$. (05 marks)

(Total 25 Marks)

Question 02

- I. What is encryption and decryption? (04 Marks)
- II. List four basic properties of good encryption algorithm. (04 Marks)
- III. What are the three (3) criteria to categorize encryption methods? (06 Marks)
- IV. Compare and contrast between Symmetric and Asymmetric key encryption algorithms. (02x03=06 Marks)
- V. Write a C++ program to encrypt a given plain text using Caesar cipher. (05 Marks)

(Total 25 Marks)

Question 03

- I. Give acronyms for the following security protocols and standards (05 Marks)
a) S/MIME b) PGP c) SET d) TLS e) SSL
- II. List two (2) security protocols to secure the Email. (04 Marks)
- III. Write the components of SET? (04 Marks)
- IV. List three (3) advantages of SET. (06 Marks)
- V. List three (3) ways to secure an Email. (06 Marks)

(Total 25 Marks)

Question 04

- I. List three (3) limitations of firewall? (03 Marks)
- II. List four (4) basic types of firewall's names. (04 Marks)
- III. Briefly describe the term malicious software. (02 Marks)
- IV. Briefly describe the two (2) categories of malicious code (04 Marks)
- V. Write the short notes for the followings (12 Marks)
a) Password capture
b) Password strength
c) Biometric authentication
d) DOS & DDOS attacks

(Total 25 Marks)

Question 05

- I. Define the following terms.
a) Digital certificate (02 Marks)
b) Digital signature (02 Marks)
- II. List out four (4) possible digital certificate types. (04 Marks)
- III. Write the contents of a "Digital Certificate"? (04 Marks)
- IV. Write the two (2) vulnerabilities in general purpose operating systems. (04 Marks)
- V. Write the security features in trusted operating systems. (04 Marks)
- VI. Define hashing in computer security and list two different hashing algorithms. (05 Marks)

(Total 25 Marks)