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 – 2018

HNDIT2301 Operating System and Computer Security

Instructions for Candidates

Answer Any Four (04) Questions Only

All question carries equal marks

No. of Questions: 05

No. of Pages : 03

Time: Two (02) hours

Question: 01

(i) Some descriptions used in information security are given below. Write suitable term among the terms given within the brackets that matches with those descriptions.
(Availability, Vulnerability, Confidentiality, Security Mechanism, Control)

a) ..... the ability of a system to ensure that an asset is viewed only by authorized parties

b) ..... the ability of a system to ensure that an asset can be used by any authorized parties

c) ..... a weak point in a system where a threat can sneak in.

d) ..... any procedure that is in place to assure security of a system.

e) ..... that is designed to detect, prevent, or recover from a security attack.

(05 Marks)

(ii) Security Attacks can be classified into two categories. Briefly explain each of them. (04 Marks)

(iii) Explain the Model for Network Security with a diagram (06 Marks)

(iv) Briefly explain the followings

a) Data integrity (02 Marks)

b) Integrity control on constrains (02 Marks)

c) Types of constraints in SQL (03 Marks)

d) Responsibilities of a DBA (03 Marks)

(Total 25 Marks)

Question: 02

(i) Briefly explain any two terms used in symmetric cipher model. (04 Marks)

(ii) Convert the following cipher text into plain text using Caser Cipher (06 Marks)

Cipher text: GRSODQ

(iii) Generate a cipher text using Rail Fence cipher (04 Marks)

Plain text: rall

(iv) Following C++ program fragment is used to convert plain text into cipher text. Fill the blanks. (06 Marks)

```
char plaintext [10];
int key =3;
cout <<"Enter Plain Text:";
cin>>plaintext;
for (int i=0; i<=sizeof(plaintext)-1; i++)
 {
cout<<char ((65+(int.....(i)....-65+....(ii)...)%...(iii)....));
 }
```

(v) Briefly explain the followings

a) Cryptography
b) Substitution Ciphers
c) One-Time Pad
d) Stream Ciphers
e) Steganography (05 Marks)

(Total 25 Marks)

Question: 03

(i) Name two uses of the following keys in Public-Key Cryptography

a) public-key
b) private-key (04 Marks)

(ii) Name any two Public-Key Applications (04 Marks)

(iii) Name the keys used for encryption and decryption process in symmetric and asymmetric encryption. (06 Marks)

(iv) List three properties of Digital Signature (06 Marks)

(v) Briefly explain what Direct Digital Signatures is. (05 Marks)

(Total 25 Marks)

Question: 04

(i) Message authentication is concerned with three reasons. List two of them. (04 Marks)

(ii) Briefly explain what Message Authentication Code (MAC) is and how it authenticates a message using a diagram. (06 Marks)

(iii) Malicious code can be classified into two types. Name them with an example for each. (04 Marks)

(iv) Briefly explain the action you should take to prevent viruses from your system. (05 Marks)

(v) There are three common non-malicious program errors. Buffer overflow is one of them. Briefly explain it and name three methods that can be used to protect from it. (06 Marks)

(Total 25 Marks)

Question: 05

Briefly explain any five (05) of the followings

(i) Classes of intruders and Intrusion Techniques.
(ii) Methods of Statistical Anomaly Detection.
(iii) Information Security Policy (ISP).
(iv) Procedure Based Access Control Vs Role Based Access Control.
(v) Five Features of Protected OS.
(vi) Variety of Web Security threats and security mechanisms.
(vii) Firewall and its limitation.
(viii) Packet Filters (explain with an image.)

(05*05marks = 25 marks)

(Total 25 Marks)