CST-303

Advanced Diploma in Information Technology (ADIT) / Bachelor in Information Technology (BIT)

Term-End Examination

December, 2007

CST-303 : INFORMATION SYSTEM SECURITY

Time : 3 Hours *Maximum Marks : 75*

Note : *There are two sections in this paper. All questions in Section A are* ***compulsory****. Answer any* ***two*** *questions from Section B.*

SECTION A

1. Virus is a *1*

(a) Database
(b) File
(c) Utility
(d) All of the above

2. There are _____ rounds in DES. *1*

(a) 16
(b) 5
(c) 14
(d) 8

3. The following is an Internet mail standard *1*

(a) SMTP
(b) FTP
(c) SNMP
(d) None of the above

4. DES encrypts blocks of _____ bits. *1*

(a) 64
(b) 128
(c) 258
(d) 32

5. RSA stands for 1

(a) Rivest Security Agency

(b) Rivest, Shamir, and Adleman

(c) Rivest Simple Algorithm

(d) None of the above

6. RSA is a 1

(a) Symmetric Key Cryptosystem

(b) Asymmetric Key Cryptosystem

(c) Public Key Cryptosystem

(d) Both (b) and (c) above

7. Cryptoanalyst is a person who 1

(a) attempts to break cryptography solutions

(b) devises cryptography solutions

(c) implements cryptography solutions

(d) None of the above

8. The four primary security principles related to a message are 1

(a) confidentiality, authentication, integrity and non-repudiation

(b) confidentiality, access control, non-repudiation and integrity

(c) authentication, authorisation, non-repudiation and availability

(d) None of the above

9. Digital Signature Certificate binds a user with 1

(a) user's passport

(b) user's driving licence

(c) user's private key

(d) user's public key

10. The following is a standard for the structure of Digital Certificate : 1

(a) X.509

(b) X.500

(c) FTP

(d) TCP/IP

11. Expand the following terms : *5*

(a) SATAN

(b) IFIP

(c) PGP

(d) MIME

(e) SMTP

12. Discuss three levels of information and computer security with suitable examples. *15*

13. Define the following terms : *15*

(a) Transposition Cipher

(b) Public Key Infrastructure

(c) Differentiate between active attack and passive attack

(d) Substitution Cipher

(e) Cryptoanalysis

SECTION B

*Answer any **two** questions from this section.*

14. Briefly describe the following terms : *15*

(a) IPSec features

(b) DNS Spoofing

(c) Integrity

(d) Digital Signature

(e) Non-repudiation

15. What do you understand by 'Authentication' and 'Encryption' in the context of system security ? Explain briefly. *15*

(a) RSA Encryption

(b) DES

(c) Kerberos

16. Write a brief note on each of the following : *15*

(a) Spoofing

(b) Trojan Horse

(c) Methods of cryptography