

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

Term-End Examination

June, 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 **three** questions from Section B.*

SECTION A

1. Fill in the blanks with words or a set of words. 15
- (i) The principle of _____ ensures that only the sender and the intended recipients have access to the contents of a message.
 - (ii) A virus program is made in such a way that it is difficult to _____.
 - (iii) _____ is the ultimate method to remove virus.
 - (iv) In _____ Brain virus marks affected sectors as bad sectors.
 - (v) DES encrypts blocks of _____ bits.
 - (vi) _____ is a person who attempts to break cryptography solutions.
 - (vii) A _____ binds a user with user's public key.
 - (viii) Conversion of plain text into cipher text is called as _____.
 - (ix) There are _____ rounds in DES.
 - (x) IPSec stands for _____.
 - (xi) _____ is a security device that allows limited access into and out of one's network.
 - (xii) _____ defines the standard for Digital Signature Certificate.
 - (xiii) _____ is an Internet Mail Standard.
 - (xiv) Another name of an anti-virus is _____.
 - (xv) _____ is gaining access by being in close tandem to authorised user.

2. (i) Expand the following terms :

10

- (a) DES
- (b) SNMP
- (c) IDEA
- (d) MUX
- (e) LFSR
- (f) FTP
- (g) PROM
- (h) FAT
- (i) SATAN
- (j) HTTP

(ii) Define the following terms :

5

- (a) Symmetric cryptography
- (b) Non-repudiation

SECTION B

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

3. (i) Describe in detail all steps in DES algorithm. 10
(ii) Discuss concept of Caesar Cipher. 5
4. What do you understand by 'Authentication' and 'Encryption' in the context of system security? In this context explain 15
(i) Kerberos
(ii) IP Security
(iii) RSA Encryption
5. Write short notes on each of the following : 15
(a) Trojan Horse
(b) Smart Cards
(c) Physical threats and security
(d) PGP
(e) Logic Bomb
6. (i) Describe the importance of digital signature in banking and insurance sector. 10
(ii) What do you understand by 'brute force attack'? 5

