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

Term-End Examination

December, 2006

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. For each of the following statements, state whether it is true or false :

(i) RSA stands for Rivest Security Agency.

(ii) DES encrypts blocks of 64 bits.

(iii) Conversion of cipher text into plain text is called as encryption.

(iv) There are sixteen rounds in DES.

(v) X.509 defines the standard for digital Signature Certificate.

(vi) Spoofing is masquerading in the reverse form.

(vii) Mathematics forms an important component of cryptography.

(viii) Worm can sabotage systems but may also perform useful tasks.

(ix) Trojan Horse is an illicit software that can infect other programs by altering them to include a copy of itself.

(x) DGP is just mail and does not perform encryption and integrity.

(xi) Kerberos is not a security tool.

(xii) Electronic access control involves electronically operated locking systems.

(xiii) Transposition is that process of enciphering in which the characters of the plain text are jumbled up into a different order according to some specific scheme.

(xiv) PROM stands for 'Programmable Read Only Memory'.

(xv) FAT keeps record of space allocated to each file in addition to keeping the directory.

2. (i) Expand the following terms :

(a) DES

(b) SATAN

(c) IFIP

(d) PGP

(e) IETF

(ii) Define the following terms :

(a) Public Key Infrastructure

(b) Differentiate between passive attack and active attack

(c) Substitution Cipher

(d) Logic Bomb

(e) Authentication

SECTION B

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

3. Describe in detail RSA algorithm. Give one example.

4. (i) Discuss the concept of Caesar cipher with suitable example and encrypt the following using shift key = +3 placed along the letter.

'CLINCH DEAL WITH CLEO'

(ii) List typical contents of a Digital Certificate.

5. (i) With the help of a diagram, describe in detail all steps in DES algorithm.

(ii) What do you understand by brute force attack ?

6. Write a brief note on each of the following :

(i) Electronic Eavesdropping

(ii) Firewall

(iii) Piggy-back Riding or Gate crashing

(iv) Data Integrity

(v) DNS spoofing