No. of Printed Pages : 4

CST-303

00674

ADIT/BIT PROGRAMME

Term-End Examination

June, 2010

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. For each of the following statements, state whether it is ***true*** or ***false*** : **15**

(a) X·509 defines the standards for Digital Signature Certificate.

(b) DES encrypts Blocks of 128 bits.

(c) Virus is an utility.

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

(e) RSA is a symmetric key Encryption

(f) Physical security can solve the virus problem to some extent.

(g) Kerberos is a security tool.

(h) RSA stands for Read Security Analyst.

(i) PGP is just a mail and does not perform encryption.

(j) SMTP is Internet Mail Standard.

(k) Caesar Cipher is an example of substitution cipher.

(l) Conversion of cipher text into plain is called as decryption.

(m) AES is Asymmetric Cipher

(n) Computer security means dealing with posting and management of security guards for computer installation.

(o) Spoofing is masquerading in reverse form.

2. (a) Describe the following : **10**

(i) Symmetric Key Cryptosystem

(ii) Hash Algorithm

(b) Describe various components of computer security. **10**

(c) Expand the following terms : **10**

(i) PEM

(ii) S/MIME

(iii) PGP

(iv) FTP

(v) TCP/IP

(vi) IPSEC

(vii) SATAN

(viii) IFIP

(ix) POP

(x) IDEA

SECTION - B

*Attempt **any two** questions from this section :*

3. Describe in detail RSA algorithm. Give one example. **15**

4. (a) List typical contents of a digital certificate. **5**

   (b) With the help of a diagram, describe all steps of DES algorithm. **10**

5. Write brief note on each of the following (3 Marks each) : **15**

   (a) Non-Repudiation

   (b) Data Integrity

   (c) Piggy - back riding

   (d) Firewall

   (e) Electronic Mail security