No. of Printed Pages : 4

CST-303

ADIT/BIT PROGRAMME

Term-End Examination

December, 2010

00615

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. **1x15=15**

   (i) DES key size is 64 bit.

   (ii) RSA is a symmetric algorithm.

   (iii) PGP is based on Asymmetric Cryptosystem .

   (iv) Digital signature binds a user with user's public key.

   (v) X. 509 defines standards for RSA algorithm.

   (vi) MIME stands for "Multipurpose. Internet Mail Extension".

(vii) Virus is a database.

(viii) FTP is an Internet Mail standard.

(ix) Cryptoanalyst is a person, who attempts to break Cryptographic solutions.

(x) Spoofing is masquerading in the reverse form.

(xi) Spam is a term used for unsolicited mail/ messages.

(xii) PEM stands for " Protection Enhanced Mail".

(xiii) Hash algorithm are also known " Message Digest or one way transformation".

(xiv) Hacker is a person who gains illegal enterance to a computer, computer system or computer resources.

(xv) Piggy-back riding means riding on back of computer system.

2. (i) What is Hash Function ? Explain with suitable example. 7

(ii) What is Digital Signature ? Explain the applications of Digital Signatures. 7

(iii) What is computer virus ? What are different possible areas of infection by viruses in a computer system ? 6

3. Expand the following Terms: 10

(a) SATAN

(b) S/MIME

(c) SMTP

(d) PEM

(e) PROM

(f) IDEA

(g) LSFR

(h) SNMP

(i) EDP

(j) S/HTTP

SECTION - B

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

4. (i) What is DOS (Denial of Service) attack ? Explain with a suitable example. **7**

   (ii) What is hacking ? What steps should be taken to protect a computer system against hacking ? **8**

5. (i) What is Cipher ? Explain different types of Ciphers with examples of each. **10**

   (ii) What is identification ? How it is different from authentication ? **5**

6. Write a brief note on each of the following : **3x5=15**

   (a) Kerberos

   (b) Firewalls

   (c) Electronic Mail Security

   (d) Digital signature certificate

   (e) DNS spoofing