* R M - 7 6 9 9 / 1 0 0 *

RM-7699

B. E. - IV (Sem. VIII) (Computer) Examination

May / June – 2010

Information Security & Application (Elective-I)

Time : **3** Hours] [Total Marks : **100**

Instructions :

(1)

નીચે દર્શાવેલ ☛ નિશાનીવાળી વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
Fillup strictly the details of ☛ signs on your answer book.

Name of the Examination :

☛ **B. E. - 4 (Sem. 8) (Computer)**

Name of the Subject :

☛ **Information Security and Application (Elective-1)**

☛ Subject Code No. : **7 6 9 9** ☛ Section No. (1, 2,.....) : **1&2**

Seat No. :

Student's Signature

(2) Use separate answer sheet for each section.
(3) Make assumption whenever required.
(4) Numbers on the right indicate marks.

SECTION-I

1 (a) Answer the following questions. Each question carried one mark : **10**

(1) Define data integrity.
(2) What is the difference between block cipher and stream cipher ?
(3) What is the block size of DES cipher ?
(4) Find out cipher text for following plain text - "welcome to vnsgu", with ceaser cipher with key=5.
(5) What is brute force attack ?
(6) What is the difference between OFB and CFB ?
(7) What is transposition cipher ?
(8) How many keys are used in triple encryption ?
(9) State true or false : Replay attack is a form of attack on data confidentiality.
(10) State true or false : Digital signature is one of the security services.

(b) (1) Define cryptanalysis and explain various cryptanalytic attacks. **4**

(2) Explain stegnography. **2**

(3) Encrypt following plaintext with vernam cipher : **4**
Plain text : 1101011101
Key : 0011111101.

OR

(3) Encrypt following plain text transposition cipher : **4**
Plain text : to get job in recession is hard
Key : 435612.

2 (a) Explain with diagram general depiction of DES encryption algorithm. **8**

(b) Explain CFB and OCB mode with diagram. **6**

OR

(b) How many S-Boxes are used in DES ? Explain the Box S-design for DES. **6**

3 Attempt the following : (any four) **16**

(1) Explain security services in detail.

(2) Explain avalanche effect of DES decryption.

(3) Explain meet-in-the middle attack of DES.

(4) Explain RC4 algorithm.

(5) Explain characteristics of link and end-to-end encryption.

SECTION-II

4 (a) Fill in the following blanks : **5**

(1) Insertion of message into the network from a fraudulent source is called _____.

(2) _____ mode provides protection to entire IP packet.

(3) _____ is an open encryption and security specification designed to protect credit card transactions on the internet.

(4) In public-key algorithm, when message was encrypted using sender's privet key, then entire encrypted message serves as a _____.

(5) A public function that maps message of any length into a fixed-length value that serves as the authenticator is called _____.

(b) Define the following : **5**

(1) Trap-door one way function

(2) Suppress replay attack

(3) Digital signature

(4) Firewall

(5) Weak-collision resistance.

(c) Attempt the followings : **10**

(1) What is public-key certificate ? What are the requirements for the use of this scheme ?

(2) Explain compression function of SHA-1.

5 Attempt any two from the followings : **14**

(1) Explain Kerberos version 4.

(2) What are the principle services provided by PGP ?

(3) What is dual signature and what is its purpose ?

6 Attempt any four from the followings : **16**

(1) Why the concept of public-key cryptography evolved ?

(2) Give the difference MD4 and MD5.

(3) List two disputes that can arise in the context of message authentication.

(4) Perform encryption and decryption for the following value using RSA algorithm :
P=3, q=11, e=7, M=5.

(5) What characteristics are needed in a secure MAC function ?

(6) Describe security policy for firewell.