* S F - 7 6 9 9 / 6 0 0 *

SF-7699

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

May / June – 2011

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

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

Seat No. :

Student's Signature

(2) Use separate answer sheet for each sections.

(3) Make assumption whenever required.

(4) Numbers on the right indicate marks.

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

(1) What is data confidentiality ?

(2) What is cryptography ?

(3) Find out cipher text for following plain text- "EXAMINATIONS", with ceaser cipher with key=4.

(4) Define the term confusion.

(5) Using which security mechanisms non repudiation can be avoided ?

(6) State true or false : Denial of service attack is an attack on confidentiality of data.

(7) State true or false : Private key cryptography is using single key for encryption and decryption both.

(8) How many keys are used in double DES ?

(9) Explain vigenere ciphers.

(10) Explain mono alphabetic cipher with example.

(b) (1) Explain how transposition techniques are used for encrypting text messages. **4**

(2) Explain rotor machine for encryption. **2**

(3) Encrypt following plaintext with hill cipher using key [3 5] [2 3] **4**

Plain text : "CRYPTOGRAPHY"

OR

(3) Encrypt following plaintext with playfair cipher with key " SCAM" plaintext : "SPECTRUM" **4**

2 (a) Explain with diagram single round of DES algorithm. **8**

(b) Write short note on cipher block chaining mode of operation in block cipher. **6**

OR

(b) Discuss triple DES with block diagram and possible attacks on it. **6**

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

(1) Explain and compare public key cryptography and private key cryptography.

(2) Explain different steganography techniques.

(3) What is the difference between differential and linear cryptanalysis ?

(4) Explain different cryptanalytic attacks on encrypted messages.

(5) Explain avalanche effect in DES.

SECTION - II

4 (a) Answer the following :

(1) What are the three broad categories of applications of public-key cryptosystems ? **2**

(2) What is the difference between weak and strong collision resistance ? **2**

(3) Explain three design goals of the firewall. **3**

(4) List out and explain the parameters that uniquely identify the security association ? **3**

(b) In context of digital signature algorithm, prove v = r. **10**

Where, $v = [(g^{u1}y^{u2}) \bmod p] \bmod q$ and $r = (g^k \bmod p) \bmod q$.

5 Answer any **two** of the following : **14**

(1) Explain transmission and reception of PGP message using flowchart.

(2) Explain SET participants with the help of figure.

(3) Explain X.509 certificate format in detail.

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

(1) Perform RSA encryption and Decryption for the following :
M = 5, p =3, q = 11 and d = 7.
(Show all necessary calculations)

(2) Explain - Dial signature.

(3) What requirements must a public-key cryptosystem fulfill to be a secure algorithm ?

(4) Consider the Diffie-Hellman scheme with q = 11 and a primitive root α =7.

(a) If user A has private Key X_A = 5, what is A's public key Y_A ?

(b) If user B has public key Y_B = 4 what is the shared secret key k ?

(5) Explain message authentication code as an authentication function.
