* R N - 7 4 4 5 / 1 0 0 *

RN-7445

B. E. - II (Sem. IV) (I.T.) Examination

May / June – 2010

Information Security & Application

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. - 2 (Sem. 4) (I.T.)

Name of the Subject :

☛ Information Security & Application

☛ Subject Code No. : 7 4 4 5 ☛ Section No. (1, 2,.....) : 1&2

Seat No. :

Student's Signature

(2) Answer to both the section must be written in **separate** answer books.

(3) Figures to the extreme right indicate maximum marks.

(4) Assume suitable data, if necessary.

(5) Support your answer with neat and clean diagram wherever necessary.

SECTION - I

1 (a) Define the following : **6**

(i) Passive Attack

(ii) Cryptology

(iii) Traffic Padding

(b) State true or False : **4**

(i) Hill Cipher is based on a 5×5 matrix of letters constructed using a keyword.

(ii) Diffie Hellman Key Exchange is based on public key cryptography.

(iii) Caesar Cipher uses a permutation of 25 alphabetic characters.

(iv) A Block cipher processes the input one block of elements at a time, producing an output block for each input block.

(c) Do as directed : **10**

(i) Explain the model for Network Security with appropraite diagram.

(ii) Describe the various types of attacks on encrypted message.

2 (a) Write short note on Triple DES. **8**

(b) Describe various Ways of Key Distribution in symmetric encryption. **7**

OR

(b) Explain RSA algorithms with example. **7**

3 (a) Describe various ways in which a hash code can be used to provide message authentication. **8**

(b) Describe Key Management in public key Cryptography. **7**

OR

(b) Compare: SHA-1 and MD5. **7**

SECTION - II

4 (a) State whether following statements are True/false. **5**

(i) Confidentiality is achieved with the help of Encryption.

(ii) The Key Used in Simplified DES has a Length of 8 bits.

(iii) One Time Pad is Unbreakable Method.

(iv) Eavesdropping on is one of the Active Attack.

(v) SET Uses Dual Signature.

(b) Fill in the blanks : **5**

(i) Cryptanalysis and cryptography together called _____.

(ii) A Possible Danger that might exploit a vulnerability in the system is known as _____.

(iii) To Counter the Replay Attacks_____ Service is used in IP Sec.

(iv) _____ establishes the Interface between SET and existing payment networks.

(v) _____ Firewall applies set of rules to each incoming IP packet.

(c) Explain simplified DES in detail with all the necessary diagrams. **10**

5 (a) Discuss Firewall Design Goals in detail. **7**

OR

(a) Discuss the parameters of Session and Connection State in Secure Socket Layer Protocol. **7**

(b) Which are the components of SET system? Explain each in brief. And also explain the steps that happen to do online shopping. **8**

OR

(b) Explain the X.509 Authentication service. Also state the elements included in X.509 certificate. **8**

6 Attempt any **three** : **15**

(i) Explain various combinations of SAs in IPSec.

(ii) Explain the Tunnel mode and Transport mode of ESP

(iii) List and explain the various applications of IPSec.

(iv) OSI Security Architecture.

(v) Cipher Feedback mode.