* S E - 7 4 4 5 / 1 0 0 *

SE-7445

B. E. IV (Sem - VII) (Information Technology) Examination

May / June – 2011

Information Security & Applications

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 - 7)**

Name of the Subject :

☛ **Information Security & Applications**

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

Seat No. :

Student's Signature

(2) Figures to the right indicate maximum marks.

(3) Assume suitable data, when necessary.

1 (a) State whether following statements are true/false : **5**

(1) In Authentication an intruder is pretending to be a legitimate user.

(2) Simplified DES is an example of asymmetric encryption technique.

(3) One Time pad is unbreakable method.

(4) Reference monitor is used to counter the Trojan Horse Attack.

(5) SET does not uses dual signature.

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

(1) Cryptanalysis and cryptography together called _____

(2) An actual attempt that exploits a vulnerability in the system is known as _____

(3) To counter the replay attacks _____ service is used in IPSec.

(4) _____ establishes the interface between SET and existing payment networks.

(5) _____ is a critical strong point in the network.

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

2 (a) Explain kerberos version 4 authentication dialogue in detail. **7**

OR

(a) Discuss in detail circuit level gateway and application level gateway. **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 SSL record protocol in detail. **8**

3 Attempt any **three** : **15**

(1) Dual signature.

(2) Explain the tunnel mode and transport mode of AH.

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

(4) Explain the format of purchase request sent by the card holder.

(5) Cipher feedback mode.

4 (a) Answer the following questions :

(1) State whether following statements are true/false : **5**

(a) RSA algorithm is public key cryptography algorithm.

(b) S-DES encryption algorithm takes 12-bits of input key.

(c) The direct digital signature involves only communicating parties.

(d) The DSA algorithm uses a symmetric cryptography method.

(e) MD5 uses a big-endian architecture.

(2) Define strong collision resistance. **1**

(3) Define Primitive root. **1**

(4) MD5 uses _____ rounds of steps in its algorithm. **1**

(5) Give full forms of the following : **2**

(a) KDC

(b) SHA - 1

(b) Answer the following :

(1) In an RSA system, the public key of a given user $e = 7$, $n = 187$. What is the private key of the user ? **6**

(2) Explain difference between MAC and Hash function. **4**

5 Answer the following questions : (any **three**) **15**

(1) Explain Diffie-Hellman key exchange with an example.

(2) Explain meet-in-the middle attack occur in double DES.

(3) Requirements for public key cryptography.

(4) Requirements for Hash functions.

6 Answer the following questions : (any **three**) **15**

(1) Explain MD5 compression functions

(2) Factoring problem in RSA algorithm

(3) Give properties of digital signatures

(4) Explain traffic confidentiality