Tot⌐No. of Questions :8]   [Total No. of Printed Pages :2

Roll No ....

IT-801
B.E. VIII Semester
Examination, June 2017
Information Security

Time : Three Hours

Maximum Marks : 70

Note: i) Eight questions are there.
     ii) Attempt five questions.
     iii) All questions carry equal marks.

1. a) Define security. What are multiple layers of security? 7
   b) Describe the critical characteristics of information. How are they used in computer security? 7

2. a) How many keys are required for two parties to communicate via a cipher? Why? 7
   b) Explain play fair cipher with suitable example. 7

3. a) Why is the middle portion of 3DES a decryption rather than an encryption? 7
   b) Explain Elliptic curve cryptography and its applications. 7

4. a) What types of attacks are addressed by message authentication? 7
   b) What basic arithmetical and logical functions are used in whirlpool? 7

736 �

IT-801   PTO

[2]

5. a) What entities constitutes a full-service kerberos environment? 7
   b) Why does PGP generate a signature before applying compression? 7

6. a) What is difference between transport mode and tunnel mode? 7
   b) Give differences among Viruses, Worms and Malware. 7

7. a) What is HTTP? How HTTP differ from HTTPS? 7
   b) List and briefly define three classes of Intruders. What is honey pot? 7

8. Write short notes on any two : 14
   a) Firewalls
   b) Eavesdropping
   c) Diffie Hellman key exchange
   d) SQL Injection

******

IT-801