Total No. of Questions 10] [Total No. of Printed Pages :1

IT - 801

B.E. VIII Semester

Examination, June 2014

Information Security

Time: Three Hours Maximum Marks: 70

Note: 1. There are ten questions with internal choice.
2. Attempt any five from them.
3. Assume missing data(if any). All questions carry equal marks.

UNIT-I

1. a) Why is confidentiality an important principle of security?
b) What is a worm? What is the significant differences between a worm and a virus?

OR

2. a) What is plaintext? Why is monoalphabetic cipher difficult to crack?
b) Distinguish between symmetric and asymmetric key cryptography?

UNIT-II

3. a) What is an Initialization Vector (IV)? What is its significance?
b) What is the important aspect that establishes trust in digital signatures?

OR

4. a) Digital envelopes combine the best features of symmetric and asymmetric key cryptography. Explain it. why?
b) Give the main differences between RSA - algorithm and Elliptic Curve Cryptography (ECC)?

UNIT-III

5. a) What is idea behind certification authority hierarchy? Why is self - signed certificate needed?
b) Why is the SSL layer positioned between the application layer and the transport layer?

OR

6. a) How does one prevent the misuse of another user's certificate in certificate - based authentication?
b) What is kerberos? How does kerberos work?

UNIT-IV

7. a) Why are some attacks called as passive? Why are other attacks called active?
b) Think and write about offering phishing - prevention techniques. Which one of them would be most effective and why?

OR

8. a) What are the two main attacks on corporate networks?
b) How can you describe SQL injection attacks? What are the techniques to prevent them? How can we overcome it?

UNTT-V

9. a) What are the limitations of a firewall? What is significance of tunnel mode?
b) How is screened host firewall, Dual - homed bastion different from screened host firewall, single homed bastion?

OR

10. a) Discuss the concept of a cookie? How can cookies damage privacy?
b) What is the role of audit records in Intrusion detection? Explain in detail?