

2124
B.E. (Information Technology)
Fifth Semester
PCIT-501: Network Security and Cryptography

Time allowed: 3 Hours

Max. Marks: 50

NOTE: Attempt five questions in all, including Question No. 1 which is compulsory and selecting two questions from each Unit.

x-x-x

1. Distinguish between the following
- a) Confidentiality Vs Privacy
 - b) Block vs Stream Ciphers
 - c) Vulnerability vs Intrusion
 - d) Threat Vs Attack
 - e) Brute Force Vs Dictionary Attack
- 5x2

UNIT - I

2. a) What are limitations of Monoalphabetic ciphers. Explain various Polyalphabetic ciphers with examples. 5
- b) Compare symmetric and asymmetric cryptography. 5
3. a) What are Public Key Certificates? What are their typical contents? 5
- b) What is Man-in-the-Middle attack? How Public Key Certificates help in defending against Man-in-the-Middle attack? 5
4. What do you mean by AES? Explain working of AES in detail. 10

UNIT - II

5. a) How symmetric key is shared over the Internet and within an enterprise? Explain with suitable diagrams. 3+5=8
- b) What do you mean by primitive root? Explain with an example. 2
6. a) What are limitations of SSL Protocols? 2
- b) What are the contents of the purchase request raised by the Customer in SET protocol? Explain the process of verifying the purchase request by merchant and Issuer. 4+2+2=8
7. Explain the architecture of IPSec in detail. Draw block diagram of Processing Model for Outbound IP Packets in IPSec. 5+5=10

x-x-x