

Note : Total Numbers of 10 questions. Attempt one from each unit. Assume missing data, if any, suitably.

Unit - I

1. a) What is system integration verification? How does verify the system? 7
- b) Why some attacks are called passive? Discuss active attacks? 7

OR

2. a) Explain the Risk Management? What are the metrics of risk management? 7
- b) How confidentiality differ from Integrity? 7

Unit - II

3. a) What is the principle of public key cryptography? 7
- b) Define cryptographic hash function? What are the properties of hash functions? 7

OR

4. a) Why, Blowfish starts with S-boxes filled with pseudorandom digits and then alters the contents using the key? 7
- b) What is the sum of three points on an elliptic curve that lie on a straight line? Explain Diffie-Hellman key exchange.

Unit - III

5. a) Define the RSA digital signature scheme and compare it to the RSA cryptosystem. 7
- b) What is network Security? What services are provided by IP security? 7

OR

6. a) What protocols comprise SSL? What is the difference between an SSL connection and an SSL session? 7
- b) What are three threats associated with user authentication over a network or Internet? 7

Unit - IV

7. a) What is the difference between an HTML filter and a WAP proxy? 7
- b) List three approaches to secure user authentication in a distributed environment. 7

OR

8. a) What is Phishing? Explain DNS based phishing. 7
- b) What is the basic difference between X.509 and PGP in terms of key hierarchies and key trust? 7

Unit - V

9. a) What is Computer Forensic? Explain the steps of forensic Investigations? 7
- b) What is the difference between transport mode and tunnel mode? Explain suicide hackers? 7

OR

10. a) What is foot printing? Explain System hacking Cycle. 7
- b) What is E mail Spider? Explain the outbound packets processing model with suitable diagram. 7