316317

25226

3 Hours / 70 Marks Seat No. | | | | | | | | |

Instructions – (1) All Questions are *Compulsory.*

(2) Answer each next main Question on a new page.

(3) Illustrate your answers with neat sketches wherever necessary.

(4) Figures to the right indicate full marks.

(5) Assume suitable data, if necessary.

(6) Use of Non-programmable Electronic Pocket Calculator is permissible.

(7) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

Marks

1. Attempt any FIVE of the following : **10**

a) State the need of computer security.

b) List any two examples of assets.

c) State any two goals of authorization.

d) Define Caesar cipher and playfair cipher.

e) State any two advantages of asymmetric cryptography.

f) What is Steganography?

g) Write any two limitations of a firewall.

Marks

2. Attempt any THREE of the following : **12**

a) Differentiate between Hotfix and Patch.

b) What is Mandatory access control (MAC) and discretionary access control (DAC).

c) Explain Simple Columnar Transposition Cipher.

d) A banking system requires fast and secure data encryption. Which is more suitable-DES or AES? Explain with reasons.

3. Attempt any THREE of the following : **12**

a) Explain spoofing attack and give it's types.

b) A company needs fast filtering with minimal processing overhead. Which firewall type is suitable? Justify your answer.

c) How does a stateful packet filter improve security compared to a packet filtering firewall in a corporate network.

d) Differentiate between PGP and S/MIME.

4. Attempt any THREE of the following : **12**

a) Explain Spyware and Adware with examples.

b) Encrypt the message 'INFORMATION' using the Rail Fence technique with 2 rails.

c) Describe how a digital signature is verified using a public key.

d) Define Honeypots and explain how they help in intrusion detection.

e) Explain the working principle of the Kerberos authentication protocol.

Marks

5. Attempt any TWO of the following : **12**

a) Explain token-based authentication. How is it different from password-based authentication.

b) Explain how plain text is converted into cipher text in a secure communication system. Illustrate with a suitable example.

c) Illustrate the roles of Authentication Server (AS) and Ticket Granting Service (TGS) with a real-time login example.

6. Attempt any TWO of the following : **12**

a) Describe Mandatory access control (MAC) and it's application in military or government system. Why is it considered more secure than discretionary access control (DAC).

b) Explain the Diffie-Hellman key exchange algorithm with a neat diagram.

c) Explain SQL Injection attack with an example.
