(6 pages) **Reg. No. :** .....

Code No. : 20327 E **Sub. Code : AECS 52**

B.Sc. (CBCS) DEGREE EXAMINATION, NOVEMBER 2022.

Fifth Semester

Computer Science

Major Elective – INTRODUCTION TO SECURITY IN COMPUTING

(For those who joined in July 2020 onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 1 = 10 marks)

Answer ALL questions.

Choose the correct answer :

1. ———— action that compromises the security of information owned by an organization.
   (a) Security attacks
   (b) Security Mechanism
   (c) Data service
   (d) Security services

2. ———— is the original intelligible message or data that is fed into the algorithm as input.
   (a) Presstext (b) PlainText
   (c) Secret Key (d) Ciphertext

3. Which of the following modes of operation in DES is used for operating?
   (a) Cipher Feedback Mode (CFB)
   (b) Cipher Block Chaining (CBC)
   (c) Electronic Code Book (ECB)
   (d) Output Feedback Modes (OFB)

4. Data encryption standard is a block cipher and encrypts data in blocks of size of ———— each.
   (a) 16 bits
   (b) 64 bits
   (c) 32 bits
   (d) All of the mentioned above

5. In SHA-3, which function does the operation L[2, 3]<- C[1] XOR L[2,3] XOR ROT(C[3],1) represent?
   (a) Theta (b) Rho
   (c) Pi (d) Chi

6. How many rounds are present in each iteration function of SHA-3?

(a) 3 (b) 4

(c) 5 (d) 6

7. There are ———— types of firewall.

(a) 5 (b) 4

(c) 3 (d) 2

8. In SHA-3, which step function does not affect W[0, 0]?

(a) Theta (b) Iota

(c) Pi (d) Chi

9. In SHA-3, for a message digest size of 256, what is the bitrate 'r' (capacity 512)?

(a) 576 (b) 1088

(c) 1152 (d) 832

10. Packet filtering firewalls are deployed on

(a) routers

(b) switches

(c) hubs

(d) repeaters

PART B — (5 × 5 = 25 marks)

Answer ALL questions, choosing either (a) or (b).
Each answer should not exceed 250 words.

11. (a) Discuss about the Active Attacks.

Or

(b) Discuss about Linear Cryptanalysis.

12. (a) What is Euler's totient function? Explain.

Or

(b) What are the principal elements of a public-key cryptosystem? – Explain.

13. (a) What is meant by Message Authentication?

Or

(b) List out the attacks during the communication across the network.

14. (a) Define Intruder. Name three different classes of intruder.

Or

(b) Define: Malicious software.

15. (a) Mention four SSL protocols.

Or

(b) What do you mean by S/MIME?

PART C — (5 × 8 = 40 marks)

Answer ALL questions, choosing either (a) or (b)
Each answer should not exceed 600 words.

16. (a) Describe about Security Services (X.800).

Or

(b) Explain about the Principles of DES.

17. (a) Describe about the Fermat's Theorem.

Or

(b) Describe about the RSA Algorithm.

18. (a) Write a detailed note on Digital signatures.

Or

(b) Compare the performance RIPEMD-160 algorithm and SHA-1 algorithm.

19. (a) Explain kerberos authentication mechanism with suitable diagram.

Or

(b) Explain about Malicious Software.

20. (a) Write a Detail notes on Intrusion Detection System.

Or

(b) Discuss about the Firewall Design Principles.

———————