

(6 pages)

Reg. No. : .....

**Code No. : 20500 E**

**Sub. Code : CECS 52**

B.Sc (CBCS) DEGREE EXAMINATION,  
NOVEMBER 2023.

Fifth Semester

Computer Science – Major Elective

**INTRODUCTION TO SECURITY IN COMPUTING**

(For those who joined in July 2021 – 2022)

Time : Three hours

Maximum : 75 marks

**PART A — (10 × 1 = 10 marks)**

Answer ALL questions.

Choose the correct answer :

1. \_\_\_\_\_ in a much less structured permutation and is much more difficult to crypt analysis.
- (a) Hill cipher
  - (b) Book cipher
  - (c) Transposition cipher
  - (d) None

2. A system for encryption and decryption is called a \_\_\_\_\_.
- (a) Plain text
  - (b) Encipher
  - (c) Cryptosystem
  - (d) Decipher
3. An Individual database and the underlying meaning of the data depends upon.
- (a) Sensitive data
  - (b) Integrated data
  - (c) Data dependency
  - (d) Coupling
4. An user tries to determine values of sensitive fields by seeking them directly with queries that yield few records called \_\_\_\_\_.
- (a) Direct attack
  - (b) Indirect attack
  - (c) DROM
  - (d) PROM
5. Which scheme provides good performance?
- (a) open addressing
  - (b) universal hashing
  - (c) hashing by division
  - (d) hasing by division
6. Digital signature needs \_\_\_\_\_ system.
- (a) Symmetric key
  - (b) Asymmetric key
  - (c) Integrity
  - (d) None

Page 2 **Code No. : 20500 E**





7. RSA algorithm is best example of \_\_\_\_\_.  
(a) Symmetric key cryptography  
(b) Asymmetric key cryptography  
(c) Elliptic curve key cryptography  
(d) None
8. To authenticate using kerberos, you must add the kerberos user principals to mongoDB to the \_\_\_\_\_ database.  
(a) \$ Internal (b) \$ External  
(c) \$ Extern (d) None
9. A more common means of virus activation is an attachment to an \_\_\_\_\_.  
(a) SMS alert (b) Down loads  
(c) E-mail message (d) Apk files
10. \_\_\_\_\_ allows unauthorized access to functionality.  
(a) Virus (b) Worm  
(c) Time bomb (d) Trapdoor

Page 3 Code No. : 20500 E

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain block cipher with neat diagram.  
Or  
(b) Write short notes on buffer overflow.
12. (a) Compare AES and DES algorithm.  
Or  
(b) Write short notes on types of malicious code with its characteristics.
13. (a) What are the different types of secure hash functions?  
Or  
(b) What are the requirements of authentication?
14. (a) What are the three types of MAC address?  
Or  
(b) Write about the importance of E-mail.
15. (a) Write about the characteristics of firewalls.  
Or  
(b) What are the security features of trusted system?

Page 4 Code No. : 20500 E

[P.T.O.]



PART C — (5 × 8 = 40 marks)

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

16. (a) Discuss about the models of Network security.

Or

- (b) Explain the function of OSI security model.

17. (a) Explain the Euler's theorem in information security.

Or

- (b) Briefly explain the RSA algorithm.

18. (a) Explain the types of authentication.

Or

- (b) What is HMAC? Difference between HMAC and MCA.

19. (a) Explain the format of X-509 authentication services.

Or

- (b) Explain with example of kerberos.

Page 5 Code No. : 20500 E

20. (a) What is Intrusion detection? Explain its types.

Or

- (b) What is cryptography? Explain its features.

Page 6 Code No. : 20500 E

