Register No.: …… Name: ……..

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

THIRD SEMESTER M.C.A DEGREE EXAMINATION (S), FEBRUARY 2023

(2020 SCHEME)

Course Code: **20MCAT221**

Course Name: **Cyber Security and Cryptography**

Max. Marks: **60** **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. List any six security mechanisms used in cryptography.
2. Explain Vigenere cipher. Encrypt '*Honesty is the best policy'* using the key '*centre*'.
3. Explain triple DES with three keys.
4. Write the principal attraction of ECC when compared with RSA.
5. List out the requirements for a good cryptographic hash function.
6. Write short note on blind signatures.
7. Explain the strategy to exploit the birthday paradox in a collision resistant attack.
8. Discuss the protocols in IPSec.
9. How can we prevent SQL injection attack?
10. What is XXE? How do you prevent it?

PART B

(Answer one full question from each module, each question carries 6 marks)

MODULE I

11. Explain the following. (6)
    i. Authentication Exchange
    ii. Traffic Padding
    iii. Access Control

OR

12. Describe playfair cipher. Find the ciphertext for the plaintext 'hide the gold in the tree stump' using the keyphrase 'playfair example'. (6)

MODULE II

13. a) Discuss RSA algorithm. (3)
    b) Encrypt the plaintext '6' using RSA. Use prime numbers 11 and 3 to calculate public key and private key. Choose smallest available integer to use assign to 'd'. Then calculate 'e'. Also, generate the cipher text using public key and do the corresponding decryption. (3)

OR

14. a) Explain Diffie Hellman key exchange algorithm. (3)

b) Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7. (3)
- If user A has private key XA=5, what is A's public key YA?
- If user B has private key XB=12, what is B's public key YB?

MODULE III

15. Explain the different applications of hash functions. (6)

OR

16. Define MAC and explain any one MAC algorithm with suitable diagram. (6)

MODULE IV

17. Explain in detail about the SSL architecture and SSL message format with suitable diagram. (6)

OR

18. Explain S/MIME protocol with various services. (6)

MODULE V

19. Elaborate on any three application security risks. (6)

OR

20. Which are the different forms of XSS? How can we prevent them? (6)

****