

Register No.: ..... Name: .....

**SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)**

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

**THIRD SEMESTER M.TECH DEGREE EXAMINATION (Regular), FEBRUARY 2022***(Telecommunication Engineering)***(2020 Scheme)****Course Code: 20ECTET221****Course Name: Secure Communication****Max. Marks: 60****Duration: 3 Hours****PART A***(Answer all questions. Each question carries 3 marks)*

1. Determine  $2^{50} \bmod 17$  using Wilson's theorem.
2. State Lagrange's theorem.
3. Perform Affine ciphering to encrypt the plain text "cryptography" using the encryption function  $E(x)=5x+8$ .
4. Discuss on AES encryption standard with a neat schematic.
5. Test whether 17 is prime or not using any one primality test algorithm.
6. Write in brief on modular exponentiation and compute  $4^{120} \bmod 11$ .
7. Use trial division algorithm to factor  $n=180$ .
8. Illustrate Fermat's algorithm for integer factorization and list its disadvantages.

**PART B***(Answer one full question from each module, each question carries 6 marks)***MODULE I**

9. Explain about complexity classes in detail. (6)

**OR**

10. Discuss about the algorithm for finding particular and general solutions of Linear Diophantine equations and also compute the solutions of  $21x + 14y = 35$ . (6)

**MODULE II**

11. Find the points on Elliptic Curve  $E_{11}(1, 6)$ . (6)

**OR**

12. Explain about algebraic structures in detail with example. (6)

**MODULE III**

13. Discuss about Linear feedback shift register. (6)

**OR**

14. Encrypt plaintext "urgent meet" using key  $k = \begin{bmatrix} 5 & 3 \\ 11 & 7 \end{bmatrix}$  using Hill cipher. (6)

**MODULE IV**

15. Apply RSA algorithm for encrypting plaintext "5" by choosing  $p=3$ ,  $q=11$ ,  $e=3$ . (6)

**OR**

16. Explain about Elliptic key cryptography in detail. (6)

**MODULE V**

17. Explain about Fermat's primality test. Does it hold true in all cases? Justify your answer with suitable example. (6)

**OR**

18. Explain about fast group operations on elliptic curve with an example. (6)

**MODULE VI**

19. Discuss about Baby step giant step algorithm. (6)

**OR**

20. Explain about any one factorization method with example. (6)

\*\*\*\*\*