Register No.: …… Name: ……..

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SECOND SEMESTER M.TECH DEGREE EXAMINATION (Regular), JULY 2022

TELECOMMUNICATION ENGINEERING

(2021 Scheme)

Course Code: **21TE205-B**

Course Name: **Secure Communication**

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

PART A

(Answer all questions. Each question carries 3 marks)

1. Detail the concept of symmetric key cryptography with a neat schematic.
2. Use the affine cipher to encrypt the message "cryptography" with the key pair (7, 2).
3. Create an LFSR with 4 cells in which the feedback function, $b_4 = b_1$ XOR b_0. Show the value of output for 5 transitions if the seed is $(0001)_2$.
4. Describe Shank's Baby-Step Giant-Step algorithm.
5. Test whether 137 is prime or not, using any one of the primality test algorithms.
6. Explain fast modular exponentiation.
7. Perform RSA algorithm choosing 17 and 11 as prime numbers to start with.
8. Explain El Gamal's public key cryptosystem with a suitable example.

PART B

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

MODULE I

9. State Euler's theorem and find the remainder when 7^8 is divided by 15. (6)

OR

10. Solve the equation $14x \equiv 12 \pmod{18}$. (6)

MODULE II

11. Discuss in detail on the algebraic structures Group, Ring and Field. (6)

OR

12. Find the gcd (161,28) using Extended Euclidean algorithm. (6)

MODULE III

13. Illustrate and explain Knapsack cryptosystem with an example. (6)

OR

14. Apply Hill cipher to encrypt the plain text "BEST OF LUCK" with the key matrix given below: (6)

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

MODULE IV

15. Elaborate on Fermat's factoring algorithm and perform the same on n = 3233. (6)

OR

16. Illustrate and explain trial division algorithm and check whether 137 is prime or not. (6)

MODULE V

17. Explain Fermat's Strong primality test with a suitable illustration. (6)

OR

18. Describe the different fast group operations on elliptic curves and determine 105P. (6)

MODULE VI

19. Explain DES encryption standard with neat schematic. (6)

OR

20. Illustrate Message Digest (MD5) algorithm with neat schematic. (6)

****