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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SIXTH SEMESTER B.TECH DEGREE EXAMINATION (R,S), MAY 2024
COMPUTER SCIENCE AND ENGINEERING
(2020 SCHEME)

Course Code : 20CST332

Course Name: Foundations of Security in Computing

Max. Marks : 100 **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. Prove the property of divisibility if a/b and a/c then a/(b+c).
2. Find the gcd (414, 662) using Euclidean algorithm.
3. Explain i) Fermat's prime
   ii) Mersenne prime.
4. Prove the congruence relation if a ≡ b (mod n) and c ≡ d (mod n) then a + c ≡ b + d (mod n) and ac ≡ bd (mod n)
5. What are Carmichael numbers. Give an example.
6. Explain Elliptic curve point algorithm.
7. How does a clickjacking attack succeed?
8. Define risk management.
9. Explain the significance of correctness and completeness in the design of operating systems.
10. Define the term security kernel.

PART B

(Answer one full question from each module, each question carries 14 marks)

MODULE I

11. a) State Euclid's algorithm for finding GCD of two numbers. Use Euclid's algorithm to find GCD (2322,654) (5)
    b) Describe the properties of:
       i) Group
       ii) Field
       iii) Rings (9)

OR

12. a) State Extended Euclid's algorithm. Using the above algorithm express gcd(252,198) as a linear combination of 252 and 198 (6)

b) Determine all solutions in the positive integers of the Diophantine equation 18x + 5y = 48. (8)

MODULE II

13. a) State and prove Fermat's theorem for primality testing. Using Fermat's theorem show that 91 is not prime. (7)

b) Use Euler's theorem to find the last two digits of 3^{256} (7)

OR

14. a) Distinguish between deterministic and probabilistic algorithms for primality testing with suitable examples. (5)

b) Explain Fermat's factorization algorithm. Use Fermat's factorization method to factor 809009. (9)

MODULE III

15. a) Solve the linear congruence equation
i)14 x ≡ 12 (mod 18)
ii) 12 x ≡ 48 (mod 18) (8)

b) Solve the simultaneous linear congruence equation:
3x + 4y ≡ 5 (mod 13)
2x + 5y ≡ 7 (mod 13) (6)

OR

16. a) For the group G = $<Z_{7^*}, x>$, find the order of the group and primitive roots in the group. (7)

b) State Chinese Remainder theorem. Solve the system of congruence, x≡2(mod 7), x ≡3(mod 9) using Chinese Remainder Theorem. (7)

MODULE IV

17. a) List and explain the countermeasures that can be taken for attacks against identification and authentication. (7)

b) Illustrate Buffer Overflow with a neat diagram and explain. (7)

OR

18. a) Explain the four aspects of malicious code infection. (10)

b) Distinguish among the terms vulnerability, threat and control. (4)

MODULE V

19. a) Explain how Operating Systems are designed for self-protection with suitable diagram showing the OS loading process. (10)

b) List any four-computer security related functions addressed by operating systems. (4)

OR

20. a) What you meant by Database Disclosure? Explain different types of Disclosures. (6)

b) How does a kernelized design support in enforcing security mechanisms? (8)

****