

Register No.: Name:

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SIXTH SEMESTER B.TECH DEGREE EXAMINATION (R), MAY 2023

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. Explain any three properties of divisibility with example.
2. Find the multiplicative inverse of 23 in Z_{100} .
3. What are the square roots of $1 \pmod{n}$ if $n=8$ (a composite number).
4. Using prime factorization method, show that *the only prime of the form $n^2 - 4$ is 5*.
5. Differentiate prime curves and binary curves.
6. Solve the equation $10x \equiv 2 \pmod{15}$.
7. Distinguish the terms vulnerability, threat and control.
8. How does a click-jacking attack succeed?
9. Describe Security Versus Precision.
10. Explain the working of two-phase update technique which helps the database manager in handling failures.

PART B

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

MODULE I

11. a) Discuss Extended Euclidian Algorithm. Using this algorithm find integers x and y such that $2173x + 2491y = 53$. (10)
- b) Determine all solutions in the +ve integers of the given Diophantine equation. (4)

$$18x + 5y = 48$$

OR

12. a) Show that for an abelian group, $(a * b)^{-1} = a^{-1} * b^{-1}$. (7)
 - b) A farmer purchased 100 heads of livestock for a total cost of Rs.4000/-. Prices were as follows; (7)
- Calves- Rs.120/-, Lambs - Rs.50/-, Piglets- Rs.25/-*

If the farmer obtained at least one animal of each type, how many of each did he buy?

MODULE II

13. a) Explain Fermat's factorization method and use this method to factor 809009. (7)
b) Explain Miller-Rabin method for primality testing. Check whether $n=61$ is prime or not using this method. (7)

OR

14. a) Define Fermat's prime. Show that any two distinct Fermat numbers are relatively prime. (7)
b) Using Pollard P-1 factorization method, find the factors of 1403. (7)

MODULE III

15. a) Solve the following system if it is solvable
$$5x + 3y \equiv 2 \pmod{14}$$
$$-3x + 4y \equiv 7 \pmod{14}$$
(7)
b) Find the general solution of the following linear congruence equation; (7)
$$14x \equiv 12 \pmod{18}$$

OR

16. a) Find an integer that has a remainder 3 when divided by 7 and 13 but is divisible by 12. (7)
b) Define Carmichael number. Show that 1729 and 2821 are Carmichael numbers. (7)

MODULE IV

17. a) Explain different E-mail attacks with necessary examples. (8)
b) List and explain the countermeasures that can be taken for attacks against identification and authentication. (6)

OR

18. a) With neat sketches explain different browser attack types. (8)
b) Illustrate Buffer Overflow with a neat diagram and explain. (6)

MODULE V

19. a) Explain the operating system tools to implement security functions. (8)
b) With neat sketches explain segmentation. (6)

OR

20. a) With necessary sketches explain paging. (8)
- b) What you meant by Database Disclosure? Explain different types of Disclosures. (6)
