

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.

20SCS14

(10 Marks)

(10 Marks)

(09 Marks)

(06 Marks)

(05 Marks)

(12 Marks)

(08 Marks)

(10 Marks)

Fig.Q4(b)

1 of 2

(10 Marks)

(10 Marks)

Module-3

- 5 a. Write extended form of Euclid's algorithm to compute GCD of two numbers. Compute the value (d, x, y) that call extended-euclid(99, 78) returns and prove that d = gcd(a, b) = ax + by (10 Marks)
 - b. Write procedure to create public and secret keys in RSA public key cryptosystem. (05 Marks)
 - c. Explain Pollard-Rho method to find factors of small numbers. (05 Marks)

OR

6	a.	Write and explain Miller-Robin primality testing.	(08 Marks)
	b.	Explain finite groups and its properties in detail.	(07 Marks)
	c.	Write and explain the Chinese Remainder Theorem.	(05 Marks)

Module-4

- 7 a. With an algorithm, explain the working procedure of Rabin Karp for string matching. Give its runtime efficiency. (10 Marks)
 - b. Explain finite automata-matcher algorithm and construct the string matching automation for the pattern P = ababaca and illustrate its operation on text string T = abababacaba (10 Marks)

OR

- 8 a. Explain Boyer-Moore algorithm for string matching and trace algorithm for the following text and pattern
 - Text : BESS_KNEW_ABOUT_BAOBABS Pattern : BAOBAB (10 Marks)
 - b. Explain Knuth Morris Pratt algorithm. Give its run-time efficiency. (10 Marks)

Module-5

9	a.	Write and explain an algorithm for polynom	ial equality testing, using Monte - Carlo method.
			(10 Marks)
	b.	Briefly explain Las Vegas algorithm.	(10 Marks)

OR

10 a. Explain randomizing deterministic algorithm taking linear search algorithm as example.

b. How to implement the dart-throwing technique using Monte - Carlo integration algorithm? Explain. (10 Marks)