U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

February / March 2023 Semester End Main Examinations

Programme: B.E.	**Semester: V**
Branch: Electronics & Telecommunication Engineering	**Duration: 3 hrs.**
Course Code: 19ET5PE1CY	**Max Marks: 100**
Course: Cryptography	**Date: 03.03.2023**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

UNIT - I

1	a)	Discuss the Challenges of Computer Security in detail.	**08**
	b)	Define attack in network security? Explain how attacks are grouped related to security goals	**06**
	c)	With a neat block diagram, discuss the functioning of network security model. List four basic tasks of designing security model.	**06**

OR

2	a)	Discuss any four Substitution Technique and list their merits and demerits.	**10**
	b)	With an example explain Reil-fence Transposition technique.	**05**
	c)	Describe the essential elements of a symmetric encryption scheme with neat diagram	**05**

UNIT - II

3	a)	Compare stream cipher and block cipher with example.	**04**
	b)	Illustrate the single round of DES encryption model with neat schematic.	**06**
	c)	State Chinese remainder theorem and find X for the given set of congruent equations using CRT $x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$.	**10**

UNIT - III

4	a)	List the different types of transformations used in AES. Discuss in detail the permutation and key-adding transformations with an Algorithm.	**10**
	b)	Elaborate block cipher modes of operation with diagrams	**10**

UNIT - IV

5	a)	Perform encryption and decryption using the RSA algorithm for the following: (a) $p = 17$, $q = 11$, $e = 7$, $M = 88$ (b) $p = 7$, $q = 11$, $e = 17$, $M = 25$	**08**

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

	b)	Briefly explain Deffie Hellman key exchange with an example and also discuss the merits and demerits of Diffie Hellman key exchange	**08**
	c)	Illustrate the PRNG (Pseudorandom) Based on RSA with neat diagram	**04**

OR

6	a)	Define Hash function with block diagram. Discuss different applications of cryptographic hash functions.	**10**
	b)	Differentiate between Message Authentication Code and Hash function.	**04**
	c)	Describe the basic Uses of Message Authentication code (MAC) in detail.	**06**

UNIT - V

7	a)	Describe Blum Blum Shub Generator with relevant equation and example	**07**
	b)	Summarize PRNG generator using block cipher with diagram	**07**
	c)	With relevant diagram explain RC4 stream generation phase	**06**

****