SVKM'S NMIMS
SCHOOL OF TECHNOLOGY MANAGEMENT& ENGINEERING, NAVI-MUMBAI

Academic Year: 2022-2023

Program: B.Tech. Stream: CSBS
Subject:Cryptology
Date:
Marks: 20

Year:2022 Semester: VII
Time: 1hr. (9:00 to10:00)
No. of Pages:1

Mid-Term Examination

Instructions: Candidates should read carefully the instructions printed on the question paper and on the cover of the Answer Book, which is provided for their use.

1) **Question No. 1 is compulsory.**
2) **Each question carries equal marks.**
3) **Answer to each new question to be started on a new page.**
4) **Figures in brackets on the right-hand side indicate full marks.**
5) **Attempt any three question from question 2 to 5.**

Q.No.	Statement of the question	CO/ SO/ BL	Marks
Q.1(a)	What is the procedude to calculate private key and public key in RSA.	BL3	(2)
Q.1 (b)	What is solution for symmetric key exchange problem.	BL3	(2)
Q.1(c)	What is the difference between symmetric key cryptography and asymmetric key cryptography.	BL1	(2)
Q.1(d)	What is stream cipher.	BL2	(2)
Q.2	What are the principles of public key cryptography.	BL1	(4)
Q.3	Explain cipher feedback mode in detail.	BL2	(4)
Q.4	Explain all the functions of round1 in AES in detail.	BL3	(4)
Q.5	What is RC4 explain in detail.	BL2	(4)

Abbreviations: Course Outcomes (CO), Students Outcomes (SO) (Refer to course policy for the details)

Guidelines for Blooms Level (BL):

Blooms Level	Type	Difficulty level	Question verbs
BL1	Remember or Understand	Low	Define, Identify, Compare, etc.
BL2	Apply or Analyze	Moderate	Solve, Illustrate, Relate, etc.
BL3	Evaluate or Create	High	Evaluate, Create, Reframe, etc.