Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

PRN: 1032210755

Mid Semester Examination

Oct 2023

CET3004B - Information and Cyber Security

Schedule ID: 21572

Faculty/School	Faculty of Engineering and Technology	**Term**	Semester V
Program	TY BTech CSE	**Duration**	**1 Hours 30 Minutes**
Specialization		**Max. Marks**	**50**

Instructions to the Candidate:

1. Write the PRN on the top right-hand corner of the question paper.
2. Draw neat diagrams.
3. Assume suitable data, if necessary.
4. Solve any 5 questions.

Section 1 (5 X 10 Marks)
Answer any 5 questions

1	A. **Explain the following with diagram: (5 M)** 1. **Interruption 2. Interception 3. Modification 4. Fabrication 5. Replay** B. Draw and explain Confidentiality, Integrity, Availability (CIA triad) with an example. (5 M)	**10 marks**	CO1, CO2	Understanding
2	A. Draw and explain the steps of each round in AES Algorithm. (5 M) B. Illustrate transposition cipher with an example (5 M)	**10 marks**	CO2, CO3, CO4	Evaluating
3	A. List and State any 5 operations inside DES algorithm. (5M) B. Compare Block Cipher and Stream Cipher. Explain in detail the block cipher modes of operations. (5 M)	**10 marks**	CO1, CO2, CO3	Analysing
4	A. Explain Chinese Remainder theorem in brief. Solve using Chinese remainder theorem (5 M) $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$ B. What is message digest? Compare MD5 and SHA-1 (5 M)	**10 marks**	CO2, CO3	Evaluating

5	A. Perform encryption and decryption using RSA algorithm. M = 5, p=11, q=3, e=7. (5M) B. What were the problems of symmetric key system, and how they are solved with RSA Public key system (5 M)	**10 marks**	CO1, CO2, CO3	Analysing
6	A. Explain in brief extended Euclidean algorithm. Find the integers x and y such that 102 x + 38 y =2 (5 M) B. List and Justify the applications of Hash Algorithms (5 M)	**10 marks**	CO1, CO2, CO3	Applying

END OF QUESTION PAPER