SOMAIYA
VIDYAVIHAR UNIVERSITY

Maximum Marks: 30	**Semester: July 2023 – Oct 2023** **Examination: In-Semester Examination**	**Duration : 1:15 hrs**
Programme code: 01 **Programme: Honors in CSF**	**Class:** SY	**Semester:** III (SVU 2020)
Name of the Constituent College: **K. J. Somaiya College of Engineering**		**Name of the department:** COMP
Course Code: 116H55C301	**Name Of The Course: Applied Cryptography**	

Question No.		**Max. Marks**	**CO Mapped**	**BT Level**
Q1	A. Define the terms vulnerability, threat and control. B. **<u>Encrypt</u>** the message "We shall overcome" using playfair cipher using the key: Understand. Assumption: Letter y and z occupy single cell in the key matrix. **OR** Consider a scenario of examination management system. Each paper has three paper setters. Each paper setter sends question to other two, when they approve, adds the question to question paper. The paper setters submit the paper to a central repository. The exam controller has access to all the papers. List and justify in one/two sentences each possible solutions to attain: A. Confidentiality (3M) B. Integrity (2M) C. Authentication of sender and receiver, both (3M) D. **LIST** Other methods of defense not covered in above scenarios(2M)	5 M 5M	CO1	RE AP
Q2	Explain working of one AES round step by step. Draw a diagram to explain logical flow of data and key elements. (You need not include contents of any P/S boxes, just explain the concept)	10	CO2	RE-UN
Q3	a. Explain the concept of Deffie-Hellman key exchange. b. Discuss vulnerabilities in the proposed approach. c. Generate a shared key for sender and receiver if: P = 23, G = 5 Alice chooses a = 4, and Bob selects b = 3.	3+2+5	CO2	AP