SY-Honors

SOMAIYA VIDYAVIHAR UNIVERSITY

Semester: January 2022 – May 2022		
Maximum Marks: 30	Examination: In-Semester Examination	Duration 1:15 hrs
Programme code: 01 Programme: B. Tech (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. Discuss How goals of security relate to acts of security harm. That is, is any of these acts equivalent to one or more of the goals? Is one of the goals encompassed by one or more of the four? B. Encrypt the message "Cryptography and System security" with playfair cipher. The encryption key is: MODERNISM and the letters a and b occupy the same position. OR Consider a scenario of electronic voting during elections. Discuss various possibilities of MOM (Motive-Opportunity-Method)	5+5 OR 10	CO1	UN AP
Q2	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen p = 17 and g = 5. i. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? ii. Is the Diffie-Hellman Key Exchange vulnerable to man in middle attack? justify your answer with an example. iii. Comment on strengths and weaknesses of Diffie-Hellman approach.	3+4+3	CO2	AP UN
Q3	A. Compare and contrast AES and DES. B. Explain the following terms with suitable examples. a. Non-Feistel cipher b. Confusion c. Diffusion	4+6	CO2	UN EV