K. J. Somaiya College of Engineering, Mumbai-77
(Autonomous College Affiliated to University of Mumbai)
Semester: **January – May 2021**
In-Semester Examination

Class: TY B. Tech
Branch: Comp. Engg. **Semester : VI**
Full name of the course: Cryptography and System Security **Course Code: 2UCC602**
Duration: 1hr.15 min (attempting questions) +15 min (uploading) **Max. Marks: 30**

Q. No	Questions	Marks
Q1	1.1 A security _____ makes use of one or more security _____ a. Service, Mechanisms b. Goal, mechanisms c. Mechanism, services d. Mechanism, goals 1.2 A student steals test question paper from a professor's office. It is an attack on which of the following a. Confidentiality b. Integrity c. Availability d. Authentication 1.3 An attacker modifies the transaction amount in banking system. It is an attack on which of the following a. Confidentiality b. Integrity c. Availability d. Authentication 1.4 State whether the following is true or false Masquerade is a passive threat. 1.5 Confusion is hiding the relationship between _____ and _____ 1.6 Diffusion is hiding the relationship between _____ and _____ 1.7 In DES algorithm the block size = ____ and key size = _____	10 marks (1 MARK EACH)

	1.8 In AES algorithm the block size = _____ and key size = _____ (all variants) 1.9 In DES algorithm, what is the probability of randomly selecting a weak, a semi-weak, or a possible weak key? 1.10 Name the modes of operation of block ciphers which allow a block cipher to be used as stream cipher	
Q2	Discuss various methods of defense giving at least one example for each method. OR A) Discuss DES algorithm analysis with respect to its strengths and weaknesses. B) You have video file with size 100 MB, Illustrate how will you send it securely using DES algorithm.	10 marks 5 marks 5 marks
Q3	A) Find the multiplicative inverse of 13 in Z_{100} using extended Euclidean method. B) With respect to below figure, prove that **L6 = L1 and R6 = R1**	05 marks 05 marks

Figure for Q3B