K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2025-26
(B. Tech) Program:Computer Engineering Scheme: IIB
Regular Examination: TY Semester: VI
Course Code: CEC602 And Course Name: Cryptography And System Security
Date of Exam: 20.05.26 Duration: 02.5 Hours Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.
(4) Scientific Calculator is not allowed.

Q. No.	Question	Max. Marks	CO	BT level
Q 1	Solve any **two** questions out of three: (05 marks each)	10		
a)	Encrypt the string "The Key is hidden under the door" using Play fair cipher where the key is "domestic"		CO1	Ap
b)	Perform encryption and decryption using the knapsack algorithm for the following X= {1,2,4,8,20,50}, W=31, M=110, Plaintext = 100101 101100 11110		CO2	Ap
c)	Explain various attacks on Digital signature.		CO4	U
Q 2	Solve any **two** questions out of three: (05 marks each)	10		
a)	Apply rail fence technique for "Savethekingfromattack"with n=3		CO1	Ap
b)	Explain ECB and CBC modes of block cipher.		CO2	U
c)	Explain UDP flood attack with its preventive measure.		CO5	U
Q.3	Solve any **two** questions out of three. (10 marks each)	20		
a)	Find the integers p and q such that 56 p + 72q = 40 and also find the GCD(56,72)		CO1	Ap
b)	i) Explain Diffie Hellman key agreement algorithm in detail.[5M] ii) Solve the following : Let Users A and B use the Diffie-Hellman key exchange technique a common prime q = 23 and a primitive root α =5 i) if user A has private key XA = 6 , what is A's public key YA? ii) if user B has private key XB = 15 , what is B's public key YB? iii) What is a shared secret key? [5M]		CO2	Ap

Seat No.:

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2025~~5~~26
(B. Tech) Program:Computer Engineering Scheme: IIB
Regular Examination: TY Semester: VI
Course Code: CEC602 And Course Name: Cryptography And System Security
Date of Exam: 20.05.26 Duration: 02.5 Hours Max. Marks: 60

c)	i) Differentiate between SHA-1 and MD5 [5M] ii) Explain cryptographic hash functions with properties of secure hash function [5M]		CO3	U
Q.4	Solve any **two** questions out of three. (10 marks each)	20		
a)	i) Describe Entity authentication Verification Categories in detail [5M] ii) Suppose Alice chooses p=7, q=13, n=91, e=5 and Message (M) =7, Find the value of the private key and verify the message using RSA digital signature scheme. [5M]		CO4	Ap
b)	Explain Secure Socket Layer (SSL) architecture in detail with a suitable diagram.		CO5	U
c)	i) Explain SQL injection and its types in detail. [5M] ii) Differentiate between Digital Signature and Conventional Signature [5M]		CO6 CO4	U

****

Seat No.: