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

Nov – Dec 2025
(B. Tech / ~~M. Tech.~~) Program: B. Tech Scheme I/II/IIB/III: IIB
Regular Examination: **LY** Semester:/VII
Course Code:AIDLC7033 and Course Name: Cryptography and Network Security
Date of Exam: 27/11/2025 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)	Apply rail fence technique for "Savethekingfromattack" with n=3		CO1	Ap
b)	Perform encryption and decryption using the RSA algorithm for the following: p=3; q=11; e=7; M=5		CO2	Ap
c)	Describe a UDP flood attack and demonstrate how it affects a target system by using an example scenario. Then, suggest and apply suitable preventive measures (such as rate limiting, firewalls, or traffic filtering) to show how the attack's impact can be reduced in practice.		CO5	Ap
Q 2	Solve any **two** questions out of three: (05 marks each)	10		
a)	Explain Security Goals and Attacks with examples. How do security services help to counter these attacks?		CO1	U
b)	Differentiate between MD5 and SHA-1		CO3	U
c)	Explain IP Spoofing attack with its Prevention.		CO5	U
Q.3	Solve any **two** questions out of three. (10 marks each)	20		
a)	Solve the following : Let Users A and B use the Diffie-Hellman key exchange technique a common prime q = 71 and a primitive root $\alpha = 7$ i) if user A has private key XA = 5 , what is As public key YA? ii) if user B has private key XB = 12 , what is Bs public key YB? iii) What is shared secret key?		CO2	Ap

Seat No.:

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

Nov – Dec 2025
(B. Tech / ~~M. Tech.~~) Program: B. Tech Scheme I/II/IIB/III: IIB
Regular Examination: **LY** Semester:/VII
Course Code:AIDLC7033 and Course Name: Cryptography and Network Security
Date of Exam: 27/11/2025 Duration: 02.5 Hours Max. Marks: 60

b)	Describe the challenge base response Authentication mechanisms with suitable diagram.		CO4	U
c)	What is DOS? Give an example of DOS? How can one protect against DOS? What is DDOS? Give an example of DDOS? How can one protect against DDOS?		CO5	U
Q.4	Solve any **two** questions out of three. (10 marks each)	20		
a)	Explain SSL architecture with suitable diagram and example		CO6	U
b)	i) State Euclids theorem and Find the GCD of 78 and 36 [5M] ii) Explain what is the purpose and working of KDC with a diagram.[5M]		CO1 CO2	U U
c)	i) Explain any 5 Properties of Secure Hash Functions [5M] ii) Explain Needham Schroeder Protocol using neat diagram [5M]		CO3 CO2	U U

****

Seat No.: