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

Program: B.Tech Scheme II Feb/March 2024
Examination: LY Semester:VII
Course Code:AIDLC7033 and Course Name:Cryptography and Network Security

Date of Exam: 01/3/2024 Duration: 2.5 Hours Max. Marks: 60

Supplementary Examination

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	**Solve any six questions out of eight:**	12		
i)	For a=86 and b=14, calculate gcd(a,b)	2	CO1	A
ii)	List the weaknesses in DES	2	CO2	U
iii)	What are block ciphers?	2	CO2	U
iv)	How will you differentiate between MD-5 and SHA	2	CO3	An
v)	Explain any three Properties of a good Hash Function	2	CO3	U
vi)	What is a digital signature? List its properties.	2	CO4	U
vii)	What is IP spoofing?	2	CO5	U
viii)	Explain the limitations and challenges in intrusion detection systems.	2	CO6	U
Q.2	**Solve any four questions out of six.**	16		
i)	Use additive Cipher with key=4 to encrypt the message “Knowledge	4	CO1	A
ii)	Compare DES and AES which one would you use and why?	4	CO2	An
iii)	Provide a comparison between Hash and MAC.	4	CO3	An
iv)	Briefly explain the purpose of a digital signature in the context of DSS.	4	CO4	An
v)	Explain TCP/IP vulnerabilities (Layer wise).	4	CO5	U
vi)	Briefly discuss the historical background of PGP and its development.	4	CO6	U

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

Program: B.Tech Scheme II Feb/March 2024
Examination: LY Semester:VII
Course Code:AIDLC7033 and Course Name:Cryptography and Network Security
Date of Exam: 01/03/2024 Duration: 2.5 Hours Max. Marks: 60

Supplementary Examination.

Q.3	**Solve any two questions out of three.**	16		
i)	Using Hill Cipher encrypt the message" we live" using the keyphrase " back up" and a 3 by 3 matrix	8	CO1	A
ii)	Write a short note on El-Gamal Algorithm.	8	CO4	U
iii)	What are the different types of firewalls and mention the layer in which they operate?	8	CO5	U
Q.4	**Solve any two questions out of three.**	16		
i)	Write a short note on knapsack algorithm	8	CO2	U
ii)	What is the need for message authentication? List various techniques used for message authentication. Explain any one	8	CO3	U
iii)	What are the different protocols in SSL? How do the client and server establish an SSL connection?	8	CO6	An

****