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

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

Date of Exam: 04/12/2023

Duration: 2.5 Hours Max. Marks: 60

		able data, if necessary.				
nA	ween single-factor and multi-factor authentication with 8 CO-	Max. Marks	СО	BT level		
Q1	Solve any six questions out of eight:	12	Write	(Gi)		
i)	Define Symmetric Cipher and Explain its Basic Operation.	2	CO1	R		
ii)	Describe the key generation process in RSA.	2	CO2	U		
iii)	Discuss how S-boxes contribute to the security of Blowfish?	2	CO2	An		
iv)	Explain the Purpose of X.509 Certificates.	2	CO3	U		
v)	Explain any three Properties of a good Hash Function	2	CO3	U		
vi)	Explain the Needham-Schroeder Authentication Protocol.	2	CO4	U		
vii) ⁹	Discuss the impact of ICMP Flood on a targeted network.	2	CO5	U		
viii)	Define SSL and TLS.	2	C06	R		
Q.2	Solve any four questions out of six.	16				
)	What is a firewall, and how does it protect a network?	4	CO1	U		
i)	Explain the basic principle of the Diffie-Hellman Key Exchange.	4	CO2	U		
ii)	Define token-based authentication. Give an example.	4	CO3	U		
v)	Briefly explain the purpose of a digital signature in the context of DSS.	4	CO4	U		
)	Explain TCP/IP vulnerabilities (Layer wise).	4	CO5	U		
i)	Briefly discuss the historical background of PGP and its development.	4	CO6	U		

EXA CNS

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

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

Date of Exam: 04/12/2023 Duration: 2.5 Hours Max. Marks: 60

Q.3	Solve any two questions out of three.	16	emolitani Li quest p	eat i
i)	Explain in detail the concept of polyalphabetic substitution.	8	CO1	U
ii)	Differentiate between single-factor and multi-factor authentication with examples.	8	CO4	An
iii)	Write a short note on ICMP flood, SYN flood, UDP flood	8	CO5	U
Q.4	Solve any two questions out of three.	16		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
i)	What are the key differences between AES and its predecessor, DES (Data Encryption Standard)?	8	CO2	U
ii)	With a block diagram, explain how you can use hashing for ensuring message integrity?	8	CO3	U
iii)	What are the main security concerns with PGP and S/MIME?	8	C06	U