

12/12/22

B

EXRL/32

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

Nov – Dec 2022

(B.Tech.) Program: Electronics and Telecommunication Engineering

Examination: TY Semester: V

Course Code: EXDLC5051 and Course Name: Data Compression and Encryption

Duration: 2.5 Hours

Max. Marks: 60

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)	Compare lossy and lossless compression.	02	1	2
ii)	Define frames in the video compression.	02	2	2
iii)	What is a security attack? Explain passive and active attacks	02	3	2
iv)	List significance of prime numbers are used in data compression.	02	4	2
v)	Define the asymmetric key cryptography.	02	5	2
vi)	Discuss the digital Immune system	02	6	2
vii)	What are the measures of performance for lossy and lossless compression techniques	02	1	2
viii)	What are the characteristics of Secure Hash Algorithms?	02	5	2
Q.2	Solve any four questions out of six.	16		
i)	Explain the LZ77 coding process in detail.	04	1	2
ii)	Explain the JPEG -2000 standard for image compression	04	2	2
iii)	Compare transposition cipher with substitution cipher.	04	3	2
iv)	State Fermat's theorem and describe its application in cryptography.	04	4	2
v)	Explain Hash function. What characteristics are needed in a secure hash function?	04	5	2

vi)	Explain system security with respect to firewalls.	04s	6	2
Q.3	Solve any two questions out of three.	16		
i)	Discuss the LZW coding and decoding technique for text compression.	08	1	2
ii)	Explain Chinese Remainder Theorem in Cryptography with suitable diagram.	08	4	2
iii)	Using the RSA algorithm, encrypt the following 1. $P=3, q=11, e=7, M=12$ 2. $P=7, q=11, e=17, M=25$ Find the corresponding ds and decrypt the cipher texts.	08	5	3
Q.4	Solve any two questions out of three.	16		
i)	Explain the μ -Law and A-Law Companding used for audio compression	08	2	2
ii)	Explain Diffie -Hellman key exchange algorithm with an example.	08	3	2
iii)	Describe biometric authentication system.	08	6	2
