



# Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India  
(Autonomous Institute Affiliated to University of Mumbai)

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
ETE701	Data Compression and Encryption	4	--	--	4	--	--	4
		Examination Scheme						
		ISE		MSE		ESE		
		10		30		100 (60% Weightage)		

<b>Pre-requisite Course Codes</b>	ETC 503 Random Signal Analysis ETC 601 Digital Communication ETC 603 Computer Communication and Networks
After successful completion of the course, student will be able to	
<b>Course Outcomes</b>	CO1 To understand the concept of Data Compression through source coding principles and various methods.
	CO2 To understand the principal of Encryption and steganography through various methods, architecture and crypto algorithm.
	CO3 To categorize and analyze various compression algorithm/standards for Text, Audio and Video.
	CO4 To identify system or data vulnerabilities and apply/design suitable crypto algorithm/mechanism to protect software/hardware configurations.

Module No.	Unit No.	Topics	Ref.	Hrs.
1	<b>Data Compression</b>		1,3,5	08
	1.1	<b>Compression Techniques:</b> Loss less compression, Lossy compression, measure of performance, modeling and coding, different types of models, and coding techniques		
	1.2	<b>Text Compression:</b> Minimum variance Huffman coding, extended Huffman coding, Adaptive Huffman coding. Arithmetic coding, Dictionary coding techniques ,LZ 77, LZ 78, LZW		
2	<b>Audio Compression</b>		1,3	04
	2.1	High quality digital audio, frequency and temporal masking, lossy sound compression, $\mu$ -law and A-law companding, and MP3 audio standard		
3	<b>Image and Video Compression</b>		3,5	12
	3.1	PCM, DPCM JPEG, JPEG –LS , and JPEG 2000 standards		
	3.2	Intra frame coding, motion estimation and compensation, introduction to MPEG -2 H-264 encoder and decoder		
4	<b>Data Security</b>		4,5	12
	4.1	Security goals, cryptography, stenography cryptographic attacks, services and mechanics.		



# Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India  
(Autonomous Institute Affiliated to University of Mumbai)

	<b>4.2</b>	Integer arithmetic, modular arithmetic, and linear congruence		
	<b>4.3</b>	Substitution cipher, transposition cipher, stream and block cipher, and arithmetic modes for block ciphers		
	<b>4.4</b>	Data encryption standard, double DES, triple DES, attacks on DES, AES, key distribution center.		
<b>5</b>	<b>Number Theory and Asymmetric Key Cryptography</b>		4,5	12
	<b>5.1</b>	Primes, factorization, Fermat's little theorem, Euler's theorem, and extended Euclidean algorithm		
	<b>5.2</b>	RSA, attacks on RSA, Diffie Hellman key exchange, key management, and basics of elliptical curve cryptography		
	<b>5.3</b>	Message integrity, message authentication, MAC, hash function, H MAC, and digital signature algorithm		
<b>6</b>	<b>System Security</b>		3,4,5	04
	<b>6.1</b>	Malware, Intruders, Intrusion detection system, firewall design, antivirus techniques, digital Immune systems, biometric authentication, and ethical hacking.		
			<b>Total</b>	<b>52</b>

## References:

1. Khalid Sayood, — *Introduction to Data Compression*|| ,Morgan Kaufmann, 2000
2. David Saloman, —*Data Compression: The complete reference*|| , Springer publication
3. Behrouz Forouzen, —*Cryptography and Network Security*|| , Tata Mc Graw –Hill Education 2011
4. Berard Menezes, —*Network Security and Cryptography*|| , learning publication Cengage
5. William Stallings, —*Cryptography and Network Security*|| , Pearson Education Asia Publication, 5th edition