Course Code	Course Name	Teaching Scheme			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
ETE701	Data Compression and Encryption	04	--	--	04	--	--	04

Course Code	Course Name	Examination Scheme							
		Theory Marks				Term Work	Practical	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Ave. Of Test 1 and Test 2					
ETE701	Data Compression and Encryption	20	20	20	80	-	-	-	100

Pre requisite :

- ETC 503 Random Signal Analysis
- ETC 601 Digital Communication
- ETC 603 Computer Communication and Networks

Course Objective: To teach the students

- Lossless and Lossy compression techniques for different types of data.
- Understand data encryption techniques
- Network security and ethical hacking.

Course Outcome : Student will able to

- Implement text, audio and video compression techniques.
- Understand symmetric and asymmetric key cryptography schemes.
- Understand network security and ethical hacking.

Module No.		Topics	Hrs.
1.		**Data Compression**	08
	1.1	**Compression Techniques:** Loss less compression, Lossy compression, measure of performance, modeling and coding, different types of models, and coding techniques	
	1.2	**Text Compression**: Minimum variance Huffman coding, extended Huffman coding, Adaptive Huffman coding. Arithmetic coding, Dictionary coding techniques ,LZ 77, LZ 78, LZW	
2		**Audio Compression**	04
	2.1	High quality digital audio, frequency and temporal masking, lossy sound compression, μ-law and A-law companding, and MP3 audio standard	
3		**Image and Video Compression**	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		**Data Security**	12
	4.1	Security goals, cryptography, stenography cryptographic attacks, services and mechanics.	
	4.2	Integer arithmetic, modular arithmetic, and linear congruence	
	4.3	Substitution cipher, transposition cipher, stream and block cipher, and arithmetic modes for block ciphers	
	4.4	Data encryption standard, double DES, triple DES, attacks on DES, AES, key distribution center.	
5		**Number Theory and Asymmetric Key Cryptography**	12
	5.1	Primes, factorization, Fermat's little theorem, Euler's theorem, and extended Euclidean algorithm	
	5.2	RSA, attacks on RSA, Diffie Hellman key exchange , key management, and basics of elliptical curve cryptography	
	5.3	Message integrity, message authentication, MAC, hash function, H MAC, and digital signature algorithm	
6		**System Security**	
	6.1	Malware, Intruders, Intrusion detection system, firewall design, antivirus techniques, digital Immune systems, biometric authentication, and ethical hacking.	04
		Total	52

Recommended Books:

1. Khalid Sayood, " *Introduction to Data Compression*" ,Morgan Kaufmann, 2000
2. David Saloman, "*Data Compression: The complete reference*" , Springer publication
3. Behrous 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

Internal Assessment (IA):
Two tests must be conducted which should cover at least 80% of syllabus. The average marks of both the test will be considered as final IA marks

End Semester Examination:
1. Question paper will comprise of 6 questions, each of 20 marks.
2. Total 4 questions need to be solved.
3. Question No.1 will be compulsory and based on entire syllabus wherein sub questions of 2 to 5 marks will be asked.
4. Remaining questions will be selected from all the modules