Course Code	Course Name	Teaching Scheme (Hrs.)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
ECCDL O5012	Data Compression and Cryptography	03	--	--	03	--	--	03

Course Code	Course Name	Examination Scheme							
		Theory Marks				Exam. Duration (in Hrs)	Term Work	Practical and Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test 2	Avg. Of Test 1 and Test 2					
ECCDL O5012	Data Compression and Cryptography	20	20	20	80	03	--	--	100

Course Objectives:

1. Gain a fundamental understanding of data compression methods for text, images, video and audio.
2. Understand the concepts of cryptography and different algorithms to provide system security.

Course Outcomes:

After successful completion of the course student will be able to

1. Apply various compression techniques for text and understand image compression and its standards.
2. Select suitable compression techniques for specified lossless and lossy audio and video applications.
3. Compare between symmetric and asymmetric cryptography and also describe different symmetric cryptographic techniques and standards.
4. Apply number theory concepts to solve the cryptographic problems.
5. Analyze different public key cryptography algorithms and also describe methods that provide the goals for integrity, confidentiality and authentication.
6. Describe system security facilities designed to protect a computer system from security threats and also appreciate ethical issues related to system security.

Module No.	Unit No.	Topics	Hrs.
1.0		**Introduction to Data Compression**	**06**
	1.1	Data compression, modelling and coding, Lossless and Lossy Compression, Arithmetic Coding – Decoding, Dictionary Based Compression, Sliding Window Compression: LZ-77, LZ-78, LZW.	
	1.2	Image Compression DCT, JPEG, JPEG – LS, Differential Lossless Compression, DPCM, JPEG – 2000 Standards.	
2.0		**Video and Audio Compression**	**06**
	2.1	Video compression: Motion compensation, temporal and spatial prediction, MPEG-4, H.264 encoder and decoder.	
	2.2	Sound, Digital Audio, μ-Law and A-Law Companding, MPEG –4 Audio Layer, Advanced Audio Coding (AAC) standard.	
3.0		**Data Security**	**10**
	3.1	Security Goals, Cryptographic Attacks and Techniques	
	3.2	Symmetric Key: Substitution Cipher, Transposition Cipher , Stream and Block Cipher	
	3.3	DES, double DES and triple DES, AES	
4.0		**Number Theory**	**04**
	4.1	Prime Numbers, Fermat's and Euler's Theorem.	
	4.2	Chinese Remainder Theorem	
5.0		**Asymmetric Key Cryptography**	**09**
	5.1	Principles of Public Key Crypto System, RSA, Key Management, Deffie-Hellman Key Exchange.	
	5.2	Message Integrity, Message Authentication and Hash Functions, SHA, HMAC, Digital Signature Standards.	
6.0		**System Security**	**04**
	6.1	Intrusion Detection System, Secure Electronic Transactions.	
	6.2	Firewall Design, Digital Immune systems, Biometric Authentication, Ethical Hacking.	
		Total	**39**

Textbooks:

1. Khalid Sayood , 3rd Edition, |Introduction to Data Compression|, Morgan Kauffman
2. Mark Nelson, Jean-Loup Gailly,IThe Data Compression Bookl, 2nd edition, BPB Publications
3. William Stallings ,|Cryptography and Network Security Principles and Practices 5th Editionl, Pearson Education.
4. Behrouz A. Forouzan, |Cryptography and Network Securityl, Tata McGraw-Hill.

Reference Books:

1. 1. David Salomon, |Data Compression: The Complete Referencel, Springer.
2. Matt Bishop, |Computer Security Art and Sciencel, Addison-Wesley.
3. Bernard Menesez,| Network Security and Cryptography| Delmar Cengage Learning, 7th Edition.

Internal Assessment (20-Marks):

Internal Assessment (IA) consists of two class tests of 20 marks each. IA-1 is to be conducted on approximately 40% of the syllabus completed and IA-2 will be based on remaining contents (approximately 40% syllabus but excluding contents covered in IA-I). Duration of each test shall be one hour. Average of the two tests will be considered as IA marks.

End Semester Examination (80-Marks):

Weightage to each of the modules in end-semester examination will be proportional to number of respective lecture hours mentioned in the curriculum.

1. Question paper will comprise of **total 06** questions, each carrying **20 marks**.
2. **Question No: 01** will be **compulsory** and based on entire syllabus wherein 4 to 5 sub-questions will be asked.
3. Remaining questions will be mixed in nature and randomly selected from all the modules.
4. Weightage of each module will be proportional to number of respective lecture hours as mentioned in the syllabus.
5. **Total 04 questions** need to be solved.