BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
Hyderabad Campus

SECOND SEMESTER 2018-2019
Course Handout Part II

Date: 7-1-2019

In addition to Part-I (General Handout for all courses appended to the timetable) this portion gives further specific details regarding the course.

Course No. : ECE F344
Course Title : Information Theory and Coding
Instructor-in-charge : P.K.Thiruvikraman

1. Course description: 3 0 3

Random variables and random processes; Information sources and source coding theorem, Kraft inequality, Shannon-Fano codes, Huffman codes, Arithmetic Codes, Lempel-Ziv-Welch algorithm, universal source codes; channel capacity: channel capacity; noisy channel coding theorem for discrete memoryless channels; error control coding: linear block codes and their properties, low density-parity-check codes, BCH codes, Reed-Solomon codes, cryptography: basic concepts on cryptography and cryptoanalysis, security issues; private-key encryption algorithms- stream ciphers, block ciphers, introduction to number theory - modular arithmetic, public-key encryption algorithms- Diffie-Hellman public-key distribution scheme, RSA public-key cryptosystem; Message authentication, digital signatures.

2. Scope & Objective:

1. To apply the concepts of random processes and probability theory to communication subsystems
2. To implement security measures in communication systems using cryptographic principles

3. Text Books

1. Information Theory, Coding and Cryptography, 3rd Ed., Dr. Ranjan Bose, Tata McGrawHill, 2016

4. Reference Books

1. Elements of information theory, Thomas M.Cover and Joy A.Thomas, Wiley-India
2. Foundations of Coding, Jiri Adamek, John Wiley, 1991
3. The Mathematics of Coding Theory, Paul Garrett, Pearson Education, 2005
4. Information Theory, Inference and Learning Algorithms, David Mackay, Cambridge University Press, 2003
5. Coding Theory – A First course, Ling and Xing, Cambridge University press, 2004

5. Course Plan

Lect. No.	Topics to be covered	Learning Objectives	Chapter in the Text Book
1-2	Introduction to Information Theory	Measure of Information	1.1 to 1.2
3-4	Average Mutual Information and Entropy	Concept of Binary Symmetric channel, conditional\l entropy	1.3
5-6	Source coding theorem	Fundamentals of source coding	1.5

7-8	Huffman Coding, Shannon-Fano-Elias Coding		1.6,1.7
9-10	Arithmetic Coding,The Lempel-Ziv algorithm, run length encoding		1.8-1.10
11-13	Introduction to Image Compression	To understand JPEG compression format and lossy compression	1.14 to 1.17
14-15	Wavelets and wavelet transform	Using the wavelet transform for compression	Class notes
16-19	Channel Capacity and Models	To understand Channel capacity & noisy coding theorem	2.1 to 2.9
20-21	Block codes for error correction	Introduction to error correcting codes	3.1 to 3.2
22-23	Matrix description of linear block codes	Parity check matrix, decoding of a linear code	3.3 to 3.6
24-25	Syndrome decoding		3.7 to 3.9
26-27	Hamming codes		3.10 to 3.16
28-29	Cyclic codes	Division algorithm for cyclic codes	4.1 to 4.3
30-33	Matrix description of cyclic codes		4.4 to 4.12
34-37	BCH codes	Generator polynomials, Minimal polynomials	5.1 to 5.10
38-40	Cryptography	Overview of encryption techniques, symmetric key cryptography,	8.1 to 8.4
41-42	Asymmetric key cryptography	The RSA algorithm	8.8 to 8.9

6. **Evaluation Scheme**

Component	Duration	Weightage	Marks	Date & Time	Nature of Component
Mid-semester test	90 min	35%	105	14/3 9.00 - 10.30AM	Open book
Programming test (MATLAB)		10%	30	TBA	Open Book
Surprise tests*	15 min	10%	30		Open Book
Comprehensive ecamination	3 hrs	45%	135	08/05 FN	Closed Book

* A total of 4 surprise tests will be conducted and the best two scores will be used.

7. **Chamber Consultation Hour**: Will be announced in the class.

8. **Notices**: Notices concerning this course will be displayed on CMS.

9. Academic Honesty and Integrity Policy: Academic honesty and integrity are to be maintained by all the students throughout the semester and no type of academic dishonesty is acceptable.

Instructor-in-Charge