Birla Institute of Technology & Science, Pilani
Hyderabad Campus

FIRST SEMESTER 2020-21
Course Handout (Part-II)

Date: 17/08/2020

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	**: Dr. Amit Ranjan Azad**

1. **Course Description: 3 0 3**
   Random Variables and Random Processes; Information Sources and Source Coding Theorem: Kraft Inequality; Huffman Coding; Shannon-Fano-Elias Coding; Arithmetic Coding; The Lempel-Ziv Algorithm; Run Length Encoding; Channel Capacity and Coding: Noisy Channel Coding Theorem; Error Control Coding; Linear Block Codes: Parity Check Matrix; Syndrome Decoding; Low Density Parity Check (LDPC) Codes; Cyclic Codes: Burst Error Correction; Bose-Chaudhuri Hocquenghem (BCH) Codes: Reed-Solomon (RS) Codes; Convolutional Codes; Trellis Coded Modulation; Cryptography: Basic Concepts of Cryptography; Security Issues; Encryption Techniques; Digital Signatures; Symmetric and Asymmetric Cryptography and Algorithms; Diffie-Hellman Key Agreement Protocol; Biometric Encryption

2. **Scope & Objective:**
   The course covers source coding, channel coding and encryption. The former deals with error correction in noisy channel, and the latter deals with secrecy of communication. Channel coding, which constitutes the major portion of the course, will introduce a number of important classes on error-detecting and error-correcting codes and their decoding. Finally, the course will give an introduction to encryption and decryption of data for secret communications.

3. **Text Book:**
   [T1] Information Theory, Coding and Cryptography, Ranjan Bose, McGraw Hill, Third Edition, 2016

4. **Reference Books:**
   [R1] Elements of Information Theory, Thomas M. Cover and Joy A. Thomas, Wiley, 1999
   [R2] Foundations of Coding, Jiri Adamek, John Wiley & Sons Inc., 1991
   [R3] The Mathematics of Coding Theory, Paul Garrett, Pearson Education, 2003
   [R4] Information Theory, Inference, and Learning Algorithms, David J. C. MacKay, Cambridge University Press, 2003
   [R5] Coding Theory: A First course, San Ling and Chaoping Xing, Cambridge University Press, 2004

5. Course Plan:

Lec. No.	Learning Objectives	Topics To Be Covered	Book
1	Introduction	Introduction, Matrices, Probability Theory	Ch-0 (T1)
2-7	Source Coding	Introduction to Information Theory, Uncertainty and Information, Average Mutual Information and Entropy, Source Coding Theorem, Huffman Coding, Shannon-Fano-Elias Coding, Arithmetic Coding, The Lempel-Ziv Algorithm, Run Length Encoding, Rate Distortion Function, Optimum Quantizer Design, Entropy Rate, Image Compression	Ch-1 (T1)
8-12	Channel Capacity and Coding	Introduction, Channel Models, Channel Capacity, Channel Coding, Information Capacity Theorem, Parallel Gaussian Channels, The Shannon Limit, Channel Capacity for MIMO Systems, Capacity Region for Multiple Access Channels	Ch-2 (T1)
13-18	Linear Block Codes for Error Correction	Introduction to Error Correcting Codes, Matrix Description of Linear Block, Equivalent Codes, Parity Check Matrix, Decoding of a Linear Block Code, Syndrome Decoding, Probability of Error Correction, Perfect Codes, Hamming Codes, Low Density Parity Check (LDPC) Codes, Optimal Linear Codes, Maximum Distance Separable (MDS) Codes, Bounds on Minimum Distance	Ch-3 (T1)
19-22	Cyclic Codes	Introduction to Cyclic Codes, Polynomials, The Division Algorithm for Polynomials, A Method for Generating Cyclic Codes, Matrix Description of Cyclic Codes, Quasi-Cyclic Codes and Shortened Cyclic Codes, Burst Error Correction, Fire Codes, Golay Codes, Cyclic Redundancy Check (CRC) Codes, Circuit Implementation of Cyclic Codes	Ch-4 (T1)
23-25	BCH Codes	Introduction to BCH Codes, Primitive Elements, Minimal Polynomials, Generator Polynomials, Examples of BCH Codes, Decoding of BCH Codes, Reed-Solomon (RS) Codes, Implementation of RS Encoders and Decoders, Performance of RS Codes Over Real Channels, Nested Codes	Ch-5 (T1)
26-28	Space-Time Codes	Introduction to Space-Time Codes, Space-Time Block Code (STBC), Space-Time Code Design Criteria, Real Orthogonal Design, Complex Orthogonal Design, STBC Design Targets and Performance	Ch-6 (T1)
29-34	Convolutional Codes	Introduction to Convolutional Codes, Tree Codes and Trellis Codes, Polynomial Description, Distance Notions, Generating Function, Matrix Description, Viterbi Decoding, Distance Bounds, Performance Bounds, Turbo Codes, Turbo Decoding, Interleaver Design for Turbo Codes	Ch-7 (T1)
35-38	Trellis Coded Modulation (TCM)	Introduction to TCM, Concept of Coded Modulation, Mapping by Set Partitioning, Ungerboeck's TCM Design Rules, TCM Decoder, Performance Evaluation for AWGN Channel, Computation of Free Euclidean Distance, TCM for Fading Channels	Ch-8 (T1)

39-42	Cryptography	Introduction to Cryptography, An Overview of Encryption Techniques, Operations used by Encryption Algorithms, Symmetric (Secret Key) Cryptography, Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RC Ciphers, Asymmetric (Public Key) Algorithms, The RSA Algorithm, Pretty Good Privacy (PGP), One-Way Hashing, Other Techniques, Elliptic Curve Cryptography, Diffie-Hellman Key Agreement Protocol, Secure Communication, Quantum Cryptography, Biometric Encryption, Cryptanalysis, Policies of Cryptography	Ch-9 (T1)

6. Evaluation Scheme:

Component	Duration	Weight	Marks	Date & Time	Evaluation Type
Test 1	30 Minutes	15%	45	September 10 – September 20 (During scheduled class hour)	Closed Book
Test 2	30 Minutes	10%	30	October 09 – October 20 (During scheduled class hour)	Closed Book
Test 3	30 Minutes	10%	30	November 10 – November 20 (During scheduled class hour)	Closed Book
Quizzes	–	10%	30	–	Closed Book
Assignments	–	20%	60	–	Open Book
Comprehensive Exam	2 Hours	35%	105	–	Closed Book
Total	–	–	300	–	–

7. Chamber Consultation Hour: To be announced in the class

8. Notices: Notices related to the course will be put up on the CMS.

9. Make-Up Examination:

No make-up will be given for Quizzes. However, for Tests and Comprehensive Exam, make-up exam will be conducted only for extremely genuine cases for which prior permission of the instructor-in-charge is required.

10. 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
ECE F344 Information Theory and Coding
Dr. Amit Ranjan Azad
Email: arazad@hyderabad.bits-pilani.ac.in
Room No.: H-240