**BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI**

**Hyderabad Campus**

**SECOND SEMESTER 2021-2022**

**Course Handout Part I**

Date: 16-01-2023

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. Atri Mukhopadhyay**

**Team of Instructors : Dr. Atri Mukhopadhyay, Dr. Sumit Kumar Chatterjee**

**1. Course description: 3 0 3**

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 crypto analysis, 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:**

The course covers source coding, channel coding & 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 of error-detecting and error-correcting codes and their decoding. Finally, the course will introduce encryption & decryption of data for secret communications.

**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 |
| 3-5 | Average Mutual Information and Entropy | Concept of Binary Symmetric channel, conditional\l entropy | 1.3 |
| 6-7 | Source coding theorem | Fundamentals of source coding | 1.6 |
| 8-9 | Huffman Coding, Shannon-Fano-Elias Coding | To introduce Universal Source coding | 1.7, 1.8 |
| 10-11 | Arithmetic Coding, The Lempel-Ziv algorithm, run length encoding, rate distortion function | To introduce optimal codes | 1.9-1.12 |
| 12-13 | Channel Capacity and Models | To understand Channel capacity & noisy coding theorem | 2.1 to 2.9 |
| 14-16 | Block codes for error correction | Introduction to error correcting codes | 3.1 to 3.2 |
| 17-20 | Matrix description of linear block codes | Parity check matrix, decoding of a linear code | 3.3 to 3.6 |
| 21 | Syndrome decoding |  | 3.7 |
| 22 | Hamming codes, LDPC |  | 3.10 to 3.11 |
| 23-25 | Cyclic codes | Division algorithm for cyclic codes | 4.1 to 4.3 |
| 26-27 | Matrix description of cyclic codes |  | 4.4 to 4.5 |
| 28-29 | BCH codes, Reed-Solomon code | Generator polynomials, Minimal polynomials | 5.1 to 5.7 |
| 30-35 | Convolutional codes, Viterbi decoding, turbo codes | To introduce the important  class of Convolutional  coder & decoder | 7.1-7.11 |
| 36-38 | Cryptography: Models, goals and early  cipher systems | Overview of encryption techniques, symmetric key cryptography, | 9.1 to 9.7 |
| 39-40 | Public Key Crypto systems and some examples Asymmetric key cryptography | The RSA algorithm | 9.8 to 9.9 |

**6. Evaluation Scheme:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Component** | **Duration** | **Weightage** | **Marks** | **Date & Time** | **Nature of Component** |
| Mid Sem | 90 mins | 30% | 90 | 18/03 2.00 - 3.30PM | Closed Book |
| Quizzes | TBA | 10% | 30 | TBA | Closed Book |
| Assignments | TBA | 20% | 60 | TBA | Open Book |
| Compre. Exam. | 180 mins | 40% | 180 | 20/05 FN | Closed Book |
| **Total** |  |  | **300** |  |  |

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

email: atrimukhopadhyay@hyderabad.bits-pilani.ac.in

8. Make-up Policy: No make-up will be given for Quizzes.However, for mid sem and Comprehensive Examination make-up examination will be given only in extremely genuine cases for which prior permission of the instructor-in-charge is required.

9. Notices: Notices, if any, concerning the course will be put up on CMS /CANVAS (will be announced in class).

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.

Atri Mukhopadhyay

**Instructor-in-charge**