Introduction to information theory, Coding and cryptography

Electrical Engineering

Instructor Name: Prof. Ranjan Bose
Institute: IIT Delhi
Department: Electrical Engineering

Course Intro: : Information theory, coding and cryptography are the three loadâ€•bearing pillars of any digital communication system. In this introductory course, we will start with the basics of information theory and source coding. Subsequently, we will discuss the theory of linear block codes (including cyclic codes, BCH codes, RS codes and LDPC codes), convolutional codes, Turbo codes, TCM and space time codes. Finally, we will introduce the basics of secure communications by focusing on cyptography and physical layer security. Wherever possible, applications of the theory in real world scenarios have been provided. The underlying aim of this course is to arouse the curiosity of the students.

Pre Requisites: : Basic exposure to linear algebra and probability theory, as well as, a course in digital communications.
Core/Elective: : Core
UG/PG: : Both
Industry Support : Telecommunication companies, Internet companies, Information security companies

Reference : Basic text book R. Bose, Information theory, coding and cryptography, McGrawâ€•Hill, 3 rd Edition, 2016.

About Instructor: Ranjan Bose received his B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT), Kanpur, India in 1992 and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania, Philadelphia, USA in 1993 and 1995, respectively. He worked at Alliance Semiconductor Inc., San Jose, CA, as a Senior Design Engineer from 1996 to 1997. Since November 1997 he has been with the Department of Electrical Engineering at Indian Institute of Technology, Delhi, where currently he is the Microsoft Chair Professor. His research interests lie in the areas of secure communications, coding theory, ultraâ€•wideband (UWB) communications, broadband wireless access and wireless security. He currently heads the Wireless Research Lab in IIT Delhi. His lectures on wireless communications form a part of the video courses offered by the National Program on Technology Enhanced Learning (NPTEL).

COURSE PLAN

SL.NO	Week	Module Name
1	1	Lecture 1: Introduction to Information Theory Lecture 2: Entropy, Mutual Information, Conditional and Joint Entropy Lecture 3: Measures for Continuous Random Variable, Relative Entropy
2	2	Lecture 4: Variable Length Codes, Prefix Codes Lecture 5: Source Coding Theorem Lecture 6: Various source coding techniques: Huffman, Arithmetic, Lempel Ziv, Run Length
3	3	Lecture 7: Optimum Quantizer, Practical Application of Source Coding: JPEG Compression Lecture 8: Introduction to Super Information Lecture 9: Channel Models and Channel Capacity
4	4	Lecture 10: Noisy Channel Coding Theorem Lecture 11: Gaussian Channel and Information Capacity Theorem Lecture 12: Capacity of MIMO channels
5	5	Lecture 13: Introduction to Error Control Coding Lecture 14: Introduction to Galois Field Lecture 15: Equivalent Codes, Generator Matrix and Parity Check Matrix
6	6	Lecture 16: Systematic Codes, Error Detections and Correction Lecture 17: Erasure and Errors, Standard Array and Syndrome Decoding Lecture 18: Probability of Error, Coding Gain and Hamming Bound
7	7	Lecture 19: Hamming Codes, LDPC Codes and MDS Codes Lecture 20: Introduction to Cyclic Codes Lecture 21: Generator Polynomial, Syndrome Polynomial and Matrix Representation
8	8	Lecture 22: Fire Code, Golay Code, CRC Codes and Circuit Implementation of Cyclic Codes Lecture 23: Introduction to BCH Codes: Generator Polynomials Lecture 24: Multiple Error Correcting BCH Codes, Decoding of BCH Codes

9	9	Lecture 25: Introduction to Reed Solomon (RS) Codes Lecture 26: Introduction to Convolutional Codes Lecture 27: Trellis Codes: Generator Polynomial Matrix and Encoding using Trellis
10	10	Lecture 28: Vitrebi Decoding and Known good convolutional Codes Lecture 29: Introduction to Turbo Codes ,Lecture 30: Introduction to Trellis Coded Modulation (TCM)
11	11	Lecture 31: Ungerboekâ€˜s design rules and Performance Evaluation of TCM schemes Lecture 32: TCM for fading channels and Space Time Trellis Codes (STTC) Lecture 33: Introduction to Space Time Block Codes (STBC)
12	12	Lecture 34: Real Orthogonal Design and Complex Orthogonal Design Lecture 35: Generalized Real Orthogonal Design and Generalized Complex Orthogonal Design Lecture 36: Introduction to Cryptography: Symmetric Key and Asymmetric Key Cryptography, Lecture 37: Some wellâ€•known Algorithms: DES, IDEA, PGP, RSA, DH Protocol Lecture 38: Introduction to Physical Layer Security: Notion of Secrecy Capacity Lecture 39: Secrecy Outage capacity, Secrecy Outage probability, Cooperative jamming