MOOCs Course on
Introduction to Information Theory, Coding and Cryptography

Instructor: Ranjan Bose, Department of Electrical Engineering, IIT Delhi

Contact: rbose.iitd@gmail.com, 9818253072, http://web.iitd.ac.in/~rbose

Duration of the course: 13 Weeks (39 Lectures)

Course Details (all 39 lectures are already recorded and available on ETSC's internal website)

Week	Topics
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	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	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	Lecture 10: Noisy Channel Coding Theorem Lecture 11: Gaussian Channel and Information Capacity Theorem Lecture 12: Capacity of MIMO channels
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	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	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	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	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	Lecture 28: Vitrebi Decoding and Known good convolutional Codes Lecture 29: Introduction to Turbo Codes

	Lecture 30: Introduction to Trellis Coded Modulation (TCM)
11	Lecture 31: Ungerboek'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	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
13	Lecture 37: Some well-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

Details of the Assignments (13 Weeks, 39 Lectures)

Week	Lesson / Topics
1	Assignment 1: MCQs based on Lectures 1 – 3
2	Assignment 2: MCQs based on Lectures 4 – 8
3	Assignment 3: MCQs based on Lectures 9 – 10
4	Assignment 4: MCQs based on Lectures 11 – 12
5	Assignment 5: MCQs based on Lectures 13 – 15
6	Assignment 6: MCQs based on Lectures 16 – 19
7	Assignment 7: MCQs based on Lectures 20 – 22
8	Assignment 8: MCQs based on Lectures 23 – 25
9	Assignment 9: MCQs based on Lectures 26 – 29
10	Assignment 10: MCQs based on Lectures 30 – 32
11	Assignment 11: MCQs based on Lectures 33 – 35
12	Assignment 12: MCQs based on Lectures 36 – 37
13	Assignment 13: MCQs based on Lectures 38 – 39

About the course

Information theory, coding and cryptography are the three load-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.

Intended Audience

This course is intended for final-year undergraduate students and first-year postgraduate students of the electrical engineering or the computer science programs. The course will help in forming a strong foundation for the broad areas of information theory, coding and cryptography. It emphasizes on the basic concepts, lays stress on the fundamental principles and motivates their application to practical problems. By design, the mathematical complexity of the course remains at a level well within the grasp of engineering college students. The course can also be used by practicing engineers as a means for a quick brush-up of the fundamentals.

Prerequisites

Basic exposure to linear algebra and probability theory, as well as, a course in digital communications.

Industries that will recognize this course

Telecommunication companies, Internet companies, Information security companies

Text Book and Reference Books

This course closely follows the text book mentioned below. Several reference books are also listed for the curious minds.

Basic text book

R. Bose, Information theory, coding and cryptography, McGraw-Hill, 3rd Edition, 2016.

Reference books for lectures 1 - 12

1. T.M. Cover and J. A. Thomas, *Elements of information theory*, John Wiley & Sons, 2012.
2. A. B. Robert, *Information Theory*, Dover Special Priced Titles, 2007.

Reference books for lectures 13 - 25

1. R. M. Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006.
2. S. Lin and D. J. Costello, *Error Control Coding*, 2nd Edition, Prentice-Hall, 2004.
3. R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2002.
4. T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, Wiley, 2005.
5. R.H. Morelos-Zaragoza, *The Art of Error Correcting Coding*, Wiley and sons, 2006.

Reference books for lectures 16 - 32

1. R. Johannesson and K.S. Zigangirov, *Fundamentals of Convolutional Coding*, 2nd Edition, Wiley-IEEE Press, 2015.
2. E. Biglieri, D. Divsalar, P.J. McLane, M.K. Simon, *Introduction to Trellis-Coded Modulation with Applications*, Macmillan, 1991.

Reference books for lectures 33 - 35

1. H. Jafarkhani, *Space-Time Coding: Theory and Practice*, Cambridge University Press, 2005.
2. B. Vucetic and J. Yuan, *Space-Time Coding*, Wiley, 2003.

Reference books for lectures 36 - 39

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th Edition, Prentice Hall, 2006.
2. B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley & Sons, 2nd Edition, 1995.
3. M. Bloch and J. Barros, *Physical-Layer Security*, Cambridge University Press, 2011.
4. R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, Springer, 2010.

About the 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, ultra-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). He is also the national coordinator for the Mission Project on Virtual Labs, which enables students all over the country to perform lab experiments remotely. He is one of the founding members of Virtualwire Technologies, a start-up company incubated within IIT Delhi. He has held guest scientist positions at the Technical University of Darmstadt, Germany, University of Colorado, Boulder, USA, UNIK, Norway and University of Maryland, Baltimore County, USA.

Dr. Bose has published over one hundred and sixty research papers in refereed journals and conferences, and filed for sixteen patents, including one granted US Patent. He received the URSI Young Scientist award in 1999, the Humboldt Fellowship in July 2000, the Indian National Academy of Engineers (INAE) Young Engineers Award in 2003, the AICTE Career Award for Young Teachers in 2004, the BOYSCAST Fellowship in 2005 and Dr. Vikram Sarabhai Research Award for the year 2013. He is the

author of the book titled *Information Theory, Coding and Cryptography* (3rd Ed.). This book has an international edition and has also been translated into Chinese and Korean. He has served as the Editor-in-Chief of IETE Journal of Education. He is presently the Associate Editor of IEEE Access and Member, Editorial Board of Computers & Security, Elsevier and the Editor of Frequenz: Journal of RF-Engineering and Telecommunications. He is a senior member of IEEE (USA) and a Fellow of IET (UK). He has been the Head of Bharti School of Telecom Technology and Management (IIT Delhi) in the past and is currently the Head of Center of Excellence in Cyber Systems and Information Assurance at IIT Delhi.

Further details and sub-topics of the Lectures (13 Weeks, 39 Lectures)

Week	1st Lecture of the week topics	2nd Lecture of the week topics	3rd Lecture of the week topics
1	▪ Uncertainty and Information ▪ Self Information ▪ Mutual Information ▪ Average Mutual Information	▪ Average Mutual Information ▪ Entropy ▪ Conditional Entropy ▪ Joint Entropy	▪ Information Measures for Continuous Random Variables ▪ Differential Entropy ▪ Average Conditional Entropy ▪ Relative Entropy (Kullback Leibler (KL) distance) ▪ Jensen Shannon distance ▪ Prefix Codes
2	▪ Variable Length Codes ▪ Kraft Inequality ▪ Source Coding Theorem ▪ Efficiency of a code	▪ Source Coding Theorem ▪ Efficiency of a code ▪ Huffman Coding ▪ Coding in blocks ▪ Examples	▪ Huffman Coding ▪ Arithmetic Coding ▪ Lempel Ziv Coding ▪ Run Length Coding ▪ Examples
3	▪ Optimum Quantizer ▪ Entropy Rate ▪ Practical Application of Source Coding ▪ JPEG Compression ▪ Examples	▪ Super Information - Motivation ▪ Background ▪ Super Information ▪ Some interesting results ▪ Conclusions	▪ Channel Models ▪ Channel Capacity ▪ Symmetric Channels ▪ Noisy Channel Coding Theorem ▪ Examples
4	▪ Channel Capacity ▪ Symmetric Channels ▪ Noisy Channel Coding Theorem ▪ Repitition Code ▪ Gaussian Channel	▪ Channel Capacity ▪ Gaussian Channel ▪ Information Capacity Theorem ▪ Shannon Limit	▪ Information Capacity Theorem ▪ Shannon Limit ▪ Capacity of MIMO channels

	▪ Examples		
5	▪ Introduction to Error Control Coding ▪ Block Codes ▪ Hamming Distance ▪ Hamming Weight ▪ Minimum Distance ▪ Examples	▪ Introduction to Error Control Coding ▪ Block Codes ▪ Hamming Distance ▪ Hamming Weight ▪ Minimum Distance ▪ Examples	▪ Linear Block Codes ▪ Equivalent Codes ▪ Generator Matrix ▪ Parity Check Matrix
6	▪ Systematic Codes ▪ Efficient Decoding ▪ Singleton Bound ▪ Maximum Distance Code ▪ Error Detections and Correction ▪ ISBN	▪ Erasure and Errors ▪ Cosets ▪ Standard Array ▪ Syndrome Decoding ▪ Examples	▪ Probability of Error ▪ Coding Gain ▪ Hamming Bound ▪ Perfect Code ▪ Examples
7	▪ Hamming Codes ▪ LDPC Codes ▪ Optimal Codes ▪ MDS Codes ▪ Examples	▪ Ring and Fields ▪ Polynomials ▪ Division Algorithm ▪ Cyclic Codes ▪ Examples	▪ Cyclic Codes ▪ Generator Polynomial ▪ Syndrome Polynomial ▪ Matrix Representation
8	▪ Generator Polynomial ▪ Fire Code, Golay Code ▪ CRC Codes ▪ Circuit Implementation ▪ Meggitt Decoder	▪ Primitive Polynomial ▪ Extenstion Field ▪ Minimal Polynomial ▪ Generator Polynomial for BCH Codes	▪ Generator Polynomial for BCH Codes ▪ Multiple Error Correcting BCH Codes ▪ Decoding of BCH Codes
9	▪ RS Codes ▪ Encoding ▪ Hardware Implementation ▪ Real Channels ▪ Nested Codes	▪ Tree Codes and Convolutional Codes ▪ Trellis Codes ▪ Encoding using Trellis ▪ Polynomial Description ▪ Generator Polynomial Matrix	▪ Tree Codes and Convolutional Codes ▪ Trellis Codes ▪ Encoding using Trellis ▪ Polynomial Description ▪ Generator Polynomial Matrix
10	▪ Matrix Description ▪ Vitrebi DecodingCodes ▪ Bounds ▪ Known good convolutional	▪ Turbo Codes ▪ Encoding ▪ Decoding ▪ Interleavers	▪ Combined Coding and Modulation ▪ Trellis Coded Modulation ▪ Free distance

	Codes ▪ Examples	▪ Examples	▪ Ungerboek's design rules ▪ Examples
11	▪ Ungerboek's design rules ▪ Performance Evaluation ▪ Examples	▪ Computation of d_{free} ▪ TCM for fading channels ▪ Space Time Trellis Codes ▪ Slow Rayleigh Fading Scenario ▪ Fast Rayleigh Fading Scenario	▪ Concept of Space Time Codes ▪ Alamouti Code ▪ Diversity ▪ Examples
12	▪ Real Orthogonal Design ▪ Generalized Real Orthogonal Design ▪ Complex Orthogonal Design ▪ Generalized Complex Orthogonal Design ▪ Examples	▪ Real Orthogonal Design ▪ Generalized Real Orthogonal Design ▪ Complex Orthogonal Design ▪ Generalized Complex Orthogonal Design ▪ Quasi Orthogonal Design ▪ Examples	▪ Introduction to Cryptography ▪ Symmetric Key ▪ Asymmetric Key ▪ Cryptanalysis
13	▪ DES ▪ IDEA ▪ PGP ▪ RSA ▪ DH Protocol	▪ Basic Concept ▪ Shannon's notion of security ▪ The wiretap model ▪ The degraded wiretap model ▪ Notion of Secrecy Capacity ▪ Wireless Scenario ▪ Examples	▪ Practical Wireless Scenario ▪ Secrecy capacity of wireless channels ▪ Outage capacity ▪ Outage probability ▪ Cooperative jamming ▪ Artificial noise forwarding ▪ Friendly jamming