# *Department of Information Technology*


School of Technology

North Eastern Hill University

Umshing, Shillong-22

# Course Structure & Syllabus

*for*

# Ph.D. Course Work

# Course Structure
# &
# Detailed Syllabus

# 1. Syllabus Scheme

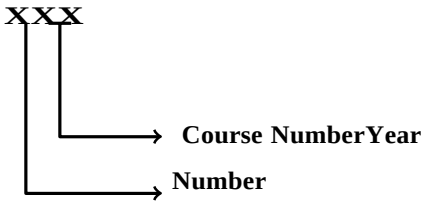
## 1.1 Coding Used in the Syllabus

**IT** - **Information Technology**

**ST** - School of Technology (For school level common papers)

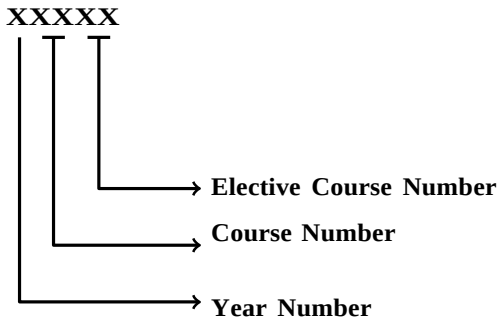
### *1.1.1* Course Coding for *Core Courses (IT-XXX)*

**Three Digit Numeric Numbers used in Course Code (e.g. IT - 500 Mathematical Foundation of Information Science):**




### 1.1.2 Course Coding for *Elective Courses (IT-XXXXX)*:

**Five Digit Numeric Numbers Used in Course Code (e.g. IT – 50201 Advanced Database Systems)**



# Course Structure

PhD Course work is a one semester course consisting of the following four papers.

**Year: I** **Semester I**

| Sl. No. | Course No. | SUBJECT | PERIODS | | | EVALUATION SCHEME | | | | | Credits |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (THEORY) | | | L | T | P | Sessional Work | | | ESE | SUB TOTAL | |
| | | | | | | TA | CT | TOT | | | |
| 1 | ST 700 | Research Methodology | 4 | 0 | 0 | 0 | 25 | 25 | 75 | 100 | 4 |
| 2 | ST 701 | Research and Publication Ethics | 2 | 0 | 0 | 0 | 12 | 12 | 38 | 50 | 2 |
| 3 | IT 702 | Algorithm Analysis and Design | 4 | 0 | 0 | 0 | 25 | 25 | 75 | 100 | 4 |
| 4 | IT 7**** | Elective | 4 | 0 | 0 | 0 | 25 | 25 | 75 | 100 | 4 |
| | Total | | 14 | - | - | - | - | 87 | 263 | 350 | 14 |

**TA**-Teachers Assessment **CT**-Class Test **ESE**-End Semester Examination Total Marks: 350
**L** – Lecture **T** – Tutorial **P** – Practical Total Periods: 14 Total Credits: 14

# Detailed Syllabus

## ST 700: Research Methodology

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

**Subject Code**: ST 700
**Subject Name**: Research Methodology.
**No. of Hours Per Week**: Lectures-4.
**Marks Distribution**: Sessional Works = 25, End Semester Examination = 75.
**Questions to be set**: Eight Questions.
**Questions to be answered**: Any Five.
**Duration of End Semester Examination**: Three Hours.

Types of Research, Research process and steps in it, Hypothesis, Research proposals and aspects.

Research Design: need, problem definition, variables, research design concepts, literature survey and review, research design process, errors in research.

Report Writing: pre-writing considerations, thesis writing, formats of report writing, formats of publications in research journals, use of standard tools like LaTeX.

**Suggested Reading**


1. Research Methodology, C.R. Kothari, 2nd Revised Edition, New Age International Publisher
2. Research Methodology, C.R. Bajpai


| L | T | P | C |
|---|---|---|---|
| 2 | 0 | 0 | 2 |

## ST 701: RESEARCH AND PUBLICATION ETHICS

**Subject Code:** ST 701
**Subject Name:** Research and Publication Ethics
**No. of Hours Per Week:** 2(Two) hours
**Marks Distribution:** Sessional Works = 12, End Semester Examination = 38.
**Questions to be set: 8** (Eight)(Question 1 is compulsory with 10 marks and remining questions would carry 7 marks each)
**Questions to be answered: Question no. 1 and any four questions from the rest**
**Duration of End Semester Examination: 2** Hours

Philosophy and ethics: Introduction to philosophy: definition, nature and scope, concept, branches, Ethics: definition, moral philosophy, nature of moral judgements and reactions
Scientific conduct: Ethics with respect to science and research, Intellectual honesty and research integrity, Scientific misconduct: Falsification, Fabrication, and Plagiarism (FFP), Redundant publications: duplicate and overlapping publications, salami slicing, Selective reporting and misrepresentation of data
Publication ethics: Publication ethics: definition, introduction and importance, Best practices / standards setting initiatives and guidelines: COPE, WAME, etc., Conflicts of interest, Publication misconduct: definition, concept, problems that lead to unethical behavior and vice versa, types, Violation of publication ethics, authorship and contributor ship, Identification of publication misconduct, complaints and appeals, Predatory publishers and journals
Open access publishing: Open access publications and initiatives, SHERPA/RoMEO online resource to check publisher copyright & self-archiving policies, Software tool to identify predatory publications developed by SPPU, Journal finder / journal suggestion tools viz. JANE, Elsevier Journal Finder, Springer Journal Suggester, etc.
Publication misconduct: Group Discussions: Subject specific ethical issues, FFP, authorship, Conflicts of interest, Complaints and appeals: examples and fraud from India and abroad, Software tools: Use of plagiarism software like Turnitin, Urkund and other open-source software tools
Databases and research metrics: Databases, Indexing databases, Citation databases: Web of Science, Scopus etc. Research Metrics: Impact Factor of journal as per Journal Citation Report, SNIP, SJR, IPP, Cite score, Metrics: h-index, g index, i10 index, altmetrics

**Suggested Readings:**


1. Bird, A. (2006). Philosophy of Science. Routledge.
2. MacIntyre, Alasdair (1967) A Short History of Ethics. London.
3. P. Chaddah, (2018) Ethics in Competitive Research: Do not get scooped; do not get plagiarized, ISBN:978_9387480865
4. National Academy of Sciences, National Academy of Engineering and Institute of Medicine.(2009). On Being a Scientist: A Guide to Responsible Conduct in Research: Third Edition. NationalAcademies Press.


**References:**


1. Resnik, D.B. (2011). What is ethics in research & why is it important. National Institute of Environmental Health Sciences,1-10. Retrieved fromhttps://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm
2. Beall, J. (2012). Predatory publishers are corrupting open access. Nature, 489(7415), 179- 179. https://doi.org/10.1038/489179a

3. Indian National Science Academy (INSA), Ethics in Science Education, Researchand Governance(2019), ISBN:978-81-939482-1-7. http://www.insaindia.res.in/pdf/Ethics_Book.pdf

## IT 702: Algorithm Analysis and Design

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

**Subject Code**: IT 702.
**Subject Name**: Algorithm Analysis and Design.
**No. of Hours Per Week**: Lectures-4.
**Marks Distribution**: Sessional Works = 25, End Semester Examination = 75.
**Questions to be set**: Eight Questions.
**Questions to be answered**: Any Five.
**Duration of End Semester Examination**: Three Hours.

Algorithms Introduction: Algorithm Design paradigms- motivation, concept of algorithmic efficiency, run time analysis of algorithms, Asymptotic Notations.

Divide and Conquer approach: Structure of divide-and-conquer algorithms: sets and disjoint sets: Union and Find algorithms, quick sort, Finding the maximum and minimum, Quick Sort, Merge sort, Heap and heap sort, the First Fourier Transform

Greedy Algorithms: Optimal storage on tapes, Knapsack problem, Job sequencing with deadlines, Minimum Spanning trees: Prim's algorithm & Kruskal's algorithm, Huffman codes.

Graph Algorithms: Representation of graphs, BFS, DFS, Topological sort, strongly connected components; single source shortest paths: Bellmen-Ford algorithm, Dijkstra's algorithm; All pairs shortest path: The Warshall's algorithm.

Dynamic programming: Overview, difference between dynamic programming and divide and conquer, Matrix chain multiplication, Traveling salesman Problem, longest Common sequence, 0/1 knapsack.

Backtracking: 8-Queen Problem, Sum of subsets, graph coloring, Hamiltonian cycles.

Branch and bound: LC searching Bounding, FIFO branch and bound, LC branch and bound application: 0/1 Knapsack problem, Traveling Salesman Problem

Linear Programming and Reductions , Introduction to Quantum algorithms.

Computational Complexity: Complexity measures, Polynomial Vs nonpolynomial time complexity; NP-hard and NP-complete classes, examples., coping with NP completeness.

**Suggested Readings**

1. E.Horowitz And S.Sahni, Fundamentals Of Computer Algorithms, Galgotia.
2. T.H.Cormen, C.E. Leiserson, R.L. Rivest, Introduction To Algorithms,The MIT Press,Cambridge
3. Vazirani, Algorithms, McGraw Hill Education Europe,2006

Subject Code: IT 7****
Subject Name: Elective
No of Hours per week: Lectures-4
Marks Distribution: Sessional Works =25, End Semester Examination=75
Question to be set: Eight Questions
Questions to be answered: Any Five
Duration of End Semester Examination: Three Hours

Any one elective course is to be selected from the list of elective courses as recommended by the supervisor or from SWAYAM courses, recommended by the supervisor and approved by the department.

**List of Elective Courses:**

| Sl. No | Name of the Elective course |
|---|---|
| 1 | IT - 70301 Advanced Wireless Networks |
| 2 | IT - 70302 Machine Learning |
| 3 | IT - 70303 Image Processing and Computer Vision |
| 4 | IT - 70401 Game Theory |
| 5 | IT - 70402 Natural Language Processing |
| 6 | IT - 70403 Computational Biology |
| 7 | IT - 70501 Quantum Computing |
| 8 | IT - 70502 Pattern Recognition |
| 9 | IT - 70503 Advanced Cryptography |

# IT - 70301 Advanced Wireless Networks

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 60001 |
| Course Name | : | *Advanced Wireless Networks* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

*Fundamentals of Wireless Networks*: Wireless Signals and its propagation in various environments, Compo- nents of Wireless Communication System, Issues of wireless communication, Cellular Networks: concepts, evolution, architecture, Issues and challenges, various communication models

*Wireless Mesh networks (WMN)*: Necessity for Mesh Networks, MAC enhancements, IEEE 802.11s Archi-tecture, Opportunistic Routing: Self Configuration and Auto Configuration

*Wireless Sensor Networks (WSN)*: Sensor Network architecture, MAC Protocols for Sensor Networks – Characteristics of MAC protocols in Sensor networks: Contention free MAC Protocols- characteristics- Traffic Adaptive Medium Access, Low energy Adaptive Clustering - Contention based MAC Protocols, Power-Aware Multi-Access protocols, Routing in Wireless Sensor Networks-Routing Challenges, Flooding, Flat Based Routing– Hierarchical Routing

*Rural Wireless Network* : Possible unique requirements for developing country users: Low-cost, Low-power, Alternative network architectures, Co-design of infrastructure and device, advantages for cost and functionality, Use of 802.11 in the developing world

## Books/References:


1. C. Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks – Architectures and Protocols", Pearson Education, 2004
2. Feng Zhao and Leonidas Guibas, "Wireless Sensor Networks", Morgan Kaufman Publishers, 2004
3. C.K.Toh, "Adhoc Mobile Wireless Networks", Pearson Education, 2002
4. Research papers.

# IT - 70302 Machine Learning

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70302 |
| Course Name | : | *Machine Learning* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

*Introduction*: Types of learning, hypothesis space and inductive bias, evaluation, cross-validation, Super- vised Learning (Regression/Classification), Distance-based methods, Nearest-Neighbours, Decision Trees, Naive Bayes, Linear Regression, Logistic Regression, Generalized Linear Models, Support Vector Machines, Nonlinearity and Kernel Methods

Unsupervised Learning, Clustering: K-means/Kernel K-means, Dimensionality Reduction: PCA and kernel PCA, Matrix Factorization and Matrix Completion, Generative Models (mixture models and latent factormodels)

Introduction to Statistical Learning Theory, Ensemble Methods, Boosting, Bagging, Random Forests, Neural Network: Perceptron, multilayer network, backpropagation.

Sparse Modeling and Estimation, Modeling Sequence/Time-Series Data, Deep Learning and Feature Representation Learning, Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Bayesian Learning.

## Books/References:


1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer2009
3. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.
4. Tom Mitchell. Machine Learning. First Edition, McGraw- Hill, 1997.
5. Ethem Alpaydin Introduction to Machine Learning, Edition 2,

# IT - 70303 Image Processing and Computer Vision

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70303 |
| Course Name | : | *Image Processing and Computer Vision.* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

Introduction to Digital Image Processing, basic concept of image formation and representation, steps in digital image processing, elements of digital image processing, relationship between pixels, image transformation.

Image enhancement: spatial domain filtering and spatial domain filtering; sharpening; contrast enhancement; restoration. Image segmentation: point; line and edge detection; thresholding; clustering; region growing. Image compression: Image Compression models; error-free compression; Lossy compression; Im- age compression standards.

Overview of Computer Vision, feature extraction in images, image classification techniques, object detection, object recognition, semantic segmentation.

Introduction to machine learning, types of machine learning techniques: supervised and unsupervised techniques. Introduction to deep learning; convolutional neural networks. Applications of machine learning in computer visions.

## Books/References:


1. Rafael C., Gonzalez Woods R.E., Digital Image Processing, Third edition, Pearson, 2013.
2. Jain A.K, Fundamentals of Digital Image Processing, Prentice Hall, Englewood Cliffs, 2002.
3. Richard Szeliski, Computer Vision: Algorithms and Applications, Springer-Verlag London Limited 2022.
4. David A. Forsyth, Jean Ponce, Computer Vision-A Modern Approach, Pearson Education, 2015.

# IT - 70401 Game Theory

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70401 |
| Course Name | : | *Game Theory* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

Introduction, overview, uses of game theory, some applications and examples, and formal definitions of: the normal form, payoffs, strategies, pure strategy Nash equilibrium, dominant strategies

Mixed-Strategy Nash Equilibrium pure and mixed strategy Nash equilibria, Iterative removal of strictly dominated strategies, minimax strategies and the minimax theorem for zero-sum game, correlated equilibria

Extensive-Form Games: Perfect information games: trees, players assigned to nodes, payoffs, backward Induction, subgame perfect equilibrium, introduction to imperfect-information games, mixed versus behavioural strategies.

Repeated Games: Repeated prisoners dilemma, finite and infinite repeated games, limited-average versus future-discounted reward, folk theorems, stochastic games and learning.

Bayesian Games: General definitions, ex ante/interim Bayesian Nash equilibrium. Coalitional Games:

Transferable utility cooperative games, Shapley value, Core, applications

## Books/References:


1. A Course in Game Theory by M. J. Osborne and A. Rubinstein, MIT Press.
2. An Introduction to Game Theory by M. J. Osborne, Oxford University Press.
3. Algorithmic Game Theory by N. Nisan, T. Rougharden, E. Tardos and V. V. Vazirani, Cambridge University Press.
4. Fun and Games: A Text on Game theory by K. Binmore, AIBS publisher

# IT - 70402 Natural Language Processing

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70402 |
| Course Name | : | *Natural Language Processing.* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

*Introduction, Text Processing, and Morphology* : Introduction to NLP, Various stages of NLP, The Ambigu- ity of Language, Parts of Speech: Nouns and Pronouns, Words: Determiners and adjectives, verbs, Phrase Structure. Character Encoding, Word Segmentation, Sentence Segmentation, Introduction to Corpora, Corpora Analysis. Inflectional and Derivation Morphology, Morphological analysis and generation using Finite State Automata and Finite State transducer.

*Language Modelling and Word Sense Disambiguatio*n: Words: Collocations, Frequency, Mean and Variance, Hypothesis testing: The t-test, Hypothesis testing of differences, Pearson's chi-square test, Likelihood ratios.Statistical Inference: N-gram Models over Sparse Data.

*Preliminaries of Disambiguation, Supervised Disambiguation* : Bayesian classification, An information the- oretic approach, Dictionary-Based Disambiguation: Disambiguation based on sense, Thesaurus-based dis- ambiguation, Disambiguation based on translations in a second-language corpus.

*Markov Model and POS Tagging: Markov Model* : Hidden Markov model, Fundamentals, Probability of properties, Parameter estimation, Variants, Multiple input observation. The Information Sources in Tag-ging: Markov model taggers, Viterbi algorithm, Applying HMMs to POS tagging, Applications of Tagging.

*Syntax and Semantics*: Shallow Parsing and Chunking, Shallow Parsing with Conditional Random Fields (CRF), Lexical Semantics, WordNet, Thematic Roles, Semantic Role Labelling with CRFs. Statistical Alignment and Machine Translation, Text alignment, Word alignment, Information extraction, Text mining, Information Retrieval, NL interfaces, Sentimental Analysis, Question Answering Systems, Social networkanalysis.

## Books/References:


1. Christopher D. Manning and Hinrich Schutze, "Foundations of Natural Language Processing", 6th Edition, The MIT Press Cambridge, Massachusetts London, England, 2003.
2. Daniel Jurafsky and James H. Martin "Speech and Language Processing", 3rd edition, Prentice Hall,2009.
3. Nitin Indurkhya, Fred J. Damerau "Handbook of Natural Language Processing", Second Edition, CRC Press, 2010.
4. James Allen, "Natural Language Understanding", Pearson Publication 8th Edition. 2012.
5. Rajesh Arumugam, Rajalingappa Shanmugamani "Hands-on natural language processing with python:A practical guide to applying deep learning architectures to your NLP application". PACKT pub- lisher, 2018

# IT - 70403 Computational Biology

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70403 |
| Course Name | : | *Computational Biology* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

Nature and scope of life science: Branches of life sciences, Characteristics of life, Levels of Organization, Origin of life, Biochemical evolution- evolution of Proteins and Nucleotide.

*Cell Biology* : The cell as basic unit of life - Prokaryotic cell and Eukaryotic cell, Cell Structure and Function- cell membrane, cell organelles, Cell Division; Mitosis Meiosis.

*Chromosome-Genome-Genes-Databases* : Bio-molecules- DNA, RNA, Protein and amino acids, Chargaff's Rules, Codon bias, GC content. Central Dogma: Replication, Transcription, Translation, Post transcriptional post translational modifications, RNA processing, RNA splicing and RNA editing. Sense/coding and anti-sense/template strands, Genetic code, wobble hypothesis. Introduction to DNA and Protein sequencing, Human Genome Project, Bioinformatics databases, Type of databases, Nucleotide sequence databases, Primary nucleotide sequence databases-EMBL, Gene Bank, DDBJ; Secondary nucleotide se- quence databases. Proteins and Databases: Protein structure and function, Protein Primary structure, Amino acid residues, Secondary, Tertiary, Quaternary Structure of Protein, Protein sequence databases-SwissProt/ TrEMBL, PIR, Sequence motif databases -Pfam, PROSITE, Protein structure databases, Protein Data Bank-SCOP, CATH, KEGG, Chembank, Sequence, structure and function relationship

*Computational Biology Algorithms*: Suffix Trees, Pair-wise alignment, Sequence Alignment Heuristics, Mul- tiple Sequence Alignment, Hidden Markov Models, RNA Secondary Structure, Bioinformatics Tools, Gene Finding, Phylogeny, Physical Mapping, Genome Rearrangements, DNA Chips and Clustering, Protein Structure, Linkage Analysis, Bayesian Networks, Stochastic Context Free Grammars, Algorithms for deep sequencing (Next Generation Sequencing), Module Identification in Networks, Expectation Maximization and Baum Welch, Gene finding and regulatory sequence analysis.

## Books/References:


1. Gerald Karp, Cell and Molecular Biology – Concepts and Experiments, 2008, Wiley InternationalStudent Version.
2. Durbin, Richard, Sean R. Eddy, et al. Biological Sequence Analysis: Probabilistic Models of Proteinsand Nucleic Acids. Cambridge University Press, 1998.

# IT - 70501 Quantum Computing

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70501 |
| Course Name | : | *Quantum Computing* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

Introduction to Quantum Computation: Quantum bits, Bloch sphere presentation of a qubit, multiple qubits.
Background Mathematics and Physics, Hilber space, Probabilities and measurements, entanglement, density operators and correlation, basics of quantum mechanics, Measurements in bases other than computational basis.
*Quantum Circuits*: single qubit gates, multiple qubit gates, design of quantum circuits. Quantum Information and Cryptography: Comparison between classical and quantum information theory. Bell states. Quantum teleportation. Quantum Cryptography, no cloning theorem.
*Quantum Algorithms*: Classical computation on quantum computers. Relationship between quantum and classical complexity classes. Deutsch's algorithm, Deutsch's-Jozsa algorithm, Shor factorization, Groversearch. Noise and error correction: Graph states and codes, Quantum error correction, fault-tolerant computation

## Books/References:


1. Quantum Computation & Quantum Information, (10th Ann Ed), by Nielsen and Chuang ISBN: 9781107002173
2. Quantum Computer Science: An Introduction, by N. D. Mermin, ISBN: 9780521876582, CAM-BRIDGE UNIV PRESS

# IT - 70502 Pattern Recognition

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

| | | |
|---|---|---|
| Course Code | : | *IT* – 70502 |
| Course Name | : | *Pattern Recognition* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours.* |

*Introduction*: Basic pattern recognition tasks; The basic structure of a pattern recognition system; Three learning paradigms; The sub-problems of pattern recognition; The nature of statistical pattern recognition; Comparing classifiers.
*Bayes Decision Theory*: General framework; Optimal decisions; Bayes maximum likelihood rule, Nearest Neighbor Classifiers Three approaches to classification: density estimation, regression and discriminant analysis;
*Feature Selection*: Algorithms for feature selection such as Branch and Bound, Sequential forward and backward selections, GSFS and GSBS, (L, R) algorithm.
*Unsupervised learning and Clustering*: Minimum within cluster distance criterion, k-means algorithm single linkage, complete linkage and average linkage algorithms etc. Principal Component Analysis

## Books/References:


1. Theodoridis and Koutroumbas, “Pattern Recognition”, Academic Press, 2009.
2. TV. S. Devi and M. N. Murty, “Pattern Recognition: An Introduction”, University Press, 2011
3. R. O. Duda, P. E. Hart and D. G. Stork, “Pattern Classification”, Wiley, 2000.

| L | T | P | C |
|---|---|---|---|
| 4 | 0 | 0 | 4 |

# IT - 70503 Advanced Cryptography

| | | |
|---|---|---|
| Course Code | : | *IT* – 602023 |
| Course Name | : | *Advanced Cryptography* |
| Contact Hours per Week | : | *4(Four) Hours.* |
| Marks Distribution | : | *Sessional Works = 40, End Semester Examination = 60.* |
| Questions to be Set | : | *Eight.* |
| Questions to be Answered | : | *Any 5(Five).* |
| Duration of End Semester Examination | : | *3(Three) Hours* |

*Introduction to Cryptography* : Basic cryptographic primitives and security issues, Secret key cryptography, public key cryptography, Hybrid cryptography. Shannon's theory on Perfect secrecy, spurious keys and unicity distance.

*Block Ciphers Stream Ciphers*: Substitution and, Permutation Network, Linear cryptanalysis: Piling -up lemma, Linear approximation of S Box. Differential cryptanalysis, Description of DES and AES, security analysis, modes of block cipher, stream ciphers: correlation attack, algebraic attack.

*Hash function and message authentication*: security of hash function: Random Oracle model, Iterated Hash Function: Merkle-damgard construction, Message Authentication Code (MAC), authenticated encryption, unconditional MAC.

*Pubic Key Cryptosystem*: RSA Cryptosystem and factoring of Integers: Primality testing, factoring of integers, Implementation of RSA: attacks on RSA, semantic security of RSA, ElGamal cryptosystem and discrete logarithmic problem: algorithms for solving discrete logarithmic problem, Elliptic curves, properties of elliptic curves , pairing on Elliptic curves, ElGamal cryptosystem on elliptic curve, security analysis of ElGamal cryptosystem,

*Signature schemes*: RSA and ElGamal signature scheme, security requirements of signature schemes Entity authentication and key distribution and agreement schemes. Post Quantum Cryptography: Introduction: lattice based, code based, multivariate and hash-based schemes.

*Miscellaneous topics*: Identity based crypto system, pallier cryptosystem, copyright protection, bitcoin and blockchain technology.

## Books/References:


1. Cryptography Theory Practice, Stinson & Paterson, CRC press, 4th Edition
2. A Handbook of Applied Cryptography, Menzes etal, CRC Press