INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KOTTAYAM

CURRICULUM AND SYLLABUS FOR THE COURSES OF B. TECH./B.TECH (HON)/DUAL DEGREE (B.TECH - MS) PROGRAMME IN COMPUTER SCIENCE AND ENGINEERING WITH SPECIALISATION IN CYBER SECURITY

Table of Contents

B.TECH./B.TECH (HON)/DUAL DEGREE (B. TECH - MS) PROGRAMME 5

SEMESTER I 6

IMA 111 Discrete Mathematics [3-1-0-4] 6

ICS 111 IT Workshop I [3-1-3-5] 6

ICS 112 Computer Programming [3-1-3-5] 7

IEC 111 Electronic Circuits and Measurements [3-1-3-5] 8

IHS 111 Communication Skills [3-0-0-3] 9

IHS 112 Foreign Language [1-0-0-1] 9

SEMESTER II 11

IMA121 Calculus and Linear Algebra [3-1-0-4] 11

IEC 121 Digital Design and Electric Circuits [3-1-3-5] 11

ICS 121 Data Structures I [3-1-3-5] 12

ICS122 Computer Organization [3-1-0-4] 13

ICS 123 IT Workshop II [2-1-3-4] 14

IHS 121 Personality Development [1-0-0-1] 14

SEMESTER III 16

IMA 211 Probability, Statistics and Random Processes [3-1-0-4] 16

ICS 211 Design and Analysis of Algorithms [3-1-0-4] 16

ICS 212 Operating Systems [3-1-0-4] 17

ICS 213 Database Management System [2-1-3-4] 18

ICS 214 IT Workshop III [2-1-3-4] 18

ISC 212 Quantum Computing and Security [2-0-0-2] 19

ICS 215 Data Structures II [1-0-3-2] 20

SEMESTER IV 21

ICS 221 Theory of Computation [3-1-0-4] 21

ICS 226 Secure Software Engineering [3-0-3-4] 21

ICS 223 Compiler Design [3-0-3-4] 22

ICS 224 Computer Networks [3-0-3-4] 23

IMA221 Differential Equations and Transforms [3-1-0-4] 23

IHS 221 Fundamentals of Economics [1-0-0-1] 24

IHS 223 Risk Management [1-0-0-1] 25

ICS 225 Data Structure III [1-0-3-2] 25

SEMESTER V 27

CBS 311 Database Security [3-0-0-3] 27

IEC 312 Distributed System Security [3-0-3-4] 27

CBS 312 Network Security, IoT and Wireless Security [3-0-3-4] 28

CBE 3311 Fundamentals of Data Science [3-0-3-4] 29

IMA 312 Number Theory and Mathematical Theory of Coding [3-0-0-3] 30

IHS 314 Financial crime, Motivations and Typologies [3-0-0-3] 31

CBE 3312 Introduction to Artificial Intelligence [1-0-0-1] 32

SEMESTER VI 33

CBS 321 Machine Learning and Cyber Security [3-0-0-3] 33

CBS 322 Digital Forensics [3-0-3-4] 33

CBE 3321 Cloud Computing and Security [3-0-3-4] 34

CBS 323 Cryptography [3-0-3-4] 35

ISC 322 Criminal Psychology and Behavior Intelligence [3-0-0-3] 35

IOE 3321 Information Security Standards, Policies, Strategies & Audits [3-0-0-3] 36

SEMESTER VII 37

CBE 4411 Mobile Forensics and Security [3-0-3-4] 37

CBS 411 Penetration Testing, Vulnerability Analysis, IDS and Malware Analysis [3-0-3-4] 37

CBS 412 Multimedia Security & Forensics [3-0-3-4] 38

IOE 4411 Block Chain & Crypto-Currencies [3-0-0-3] 39

SEMESTER VIII 40

CBE 4421 Cyber Ethics, Privacy and Legal Issues [3-0-0-3] 40

CBE 4422 Biometric Security [3-0-3-4] 40

IOE 4421 Lightweight Cryptography [3-0-0-3] 41

BTech-MS Course Structure for Computer Science and Engineering with Specialisation In Cyber Security

Semester –I						Semester -II					
Course	**Course Name**	**L**	**T**	**P**	**C**	**Course**	**Course Name**	**L**	**T**	**P**	**C**
IMA 111	Discrete Mathematics	3	1	0	4	IMA 121	Calculus and Linear Algebra	3	1	0	4
ICS 111	IT Workshop I	3	1	3	5	IEC 121	Digital Design and Electric Circuits	3	1	3	5
ICS 112	Computer Programming	3	1	3	5	ICS 121	Data Structures I	3	1	3	5
IEC 111	Electronic Circuits and Measurements	3	1	3	5	ICS 122	Computer Organization	3	1	0	4
IHS 111	Communication Skills	3	0	0	3	ICS 123	IT Workshop II	2	1	3	4
IHS 112	Foreign Language	1	0	0	1	IHS 121	Personality Development	1	0	0	1
IPT 111	Physical Training I	0	0	2	0						
Total		**16**	**4**	**11**	**23**	**Total**		**15**	**5**	**9**	**23**
Cumulative Credits at the End of First Year: 46											
Semester –III						**Semester -IV**					
Course	**Course Name**	**L**	**T**	**P**	**C**	**Course**	**Course Name**	**L**	**T**	**P**	**C**
IMA 211	Probability, Statistics and Random Processes	3	1	0	4	ICS 221	Theory of Computation	3	1	0	4
ICS 211	Design and Analysis of Algorithms	3	1	0	4	ICS 226	Secure Software Engineering	3	0	3	4
ICS 212	Operating Systems	3	1	0	4	ICS 223	Compiler Design	3	0	3	4
ICS 213	Databases Management Systems	2	1	3	4	ICS 224	Computer Networks	3	0	3	4
ICS 214	IT Workshop III	2	1	3	4	IMA 221	Differential Equations and Transforms	3	1	0	4
ISC 212	Quantum Computing and Security	2	0	0	2	IHS 221	Fundamentals of Economics	1	0	0	1
ICS 215	Data Structures II	1	0	3	2	IHS 223	Risk Management	1	0	0	1
IPT 211	Physical Training II	0	0	2	0	ICS 225	Data Structures III	1	0	3	2
Total		**16**	**5**	**11**	**24**	**Total**		**18**	**2**	**12**	**24**
Cumulative Credits at the End of Second Year: 94											
Semester –V						**Semester -VI**					
Course	**Course Name**	**L**	**T**	**P**	**C**	**Course**	**Course Name**	**L**	**T**	**P**	**C**
CBS 311	Database Security	3	0	0	3	CBS 321	Machine Learning and Cyber Security	3	0	0	3
IEC 312	Distributed System Security	3	0	3	4	CBS 322	Digital Forensics	3	0	3	4
CBS 312	Network Security, IoT and Wireless Security	3	0	3	4	CBE 3321	Cloud Computing and Security	3	0	3	4
CBE 3311	Fundamentals of Data Science	3	0	3	4	CBS 323	Cryptography	3	0	3	4
IMA 312	Number Theory and Mathematical Theory of Coding	3	0	0	3	ISC 322	Criminal Psychology and Behavior Intelligence	3	0	0	3
IHS 314	Financial crime, Motivations and Typologies	3	0	0	3	IOE 3321	Information Security Standards, Policies, Strategies & Audits	3	0	0	3
CBE 3312	Introduction to Artificial Intelligence	1	0	0	1	CBS 225	Honours Project I (Optional) I				
Total		**18**	**0**	**12**	**22**	**Total**		**18**	**0**	**9**	**21**
Cumulative Credits at the End of Third Year: 137											
Semester –VII						**Semester -VIII**					
Course	**Course Name**	**L**	**T**	**P**	**C**	**Course**	**Course Name**	**L**	**T**	**P**	**C**
CBE 4411	Mobile Forensics and Security	3	0	3	4	CBE 4421	Cyber Ethics, Privacy and Legal Issues	3	0	0	3
CBS 411	Penetration Testing, Vulnerability Analysis, IDS and Malware Analysis	3	0	3	4	CBE 4422	Biometric Security / Industrial Training	3	0	3	4
CBS 412	Multimedia Security & Forensics	3	0	3	4	IOE 4421	Lightweight Cryptography	3	0	0	3
IOE 4411	Block Chain & Crypto-Currencies	3	0	0	3	CBS 423	BTP - II	6	0	0	6
CBS 413	BTP - I	6	0	0	6	CBS 425	Honours Project II (Optional)				
ICB XXX	Research Course (Optional)					ICB XXX	Research Course (Optional)				
Total		**18**	**0**	**9**	**21**	**Total**		**15**	**0**	**3**	**16**
Cumulative Credits at the End of Fourth Year:174(BTech); 174+ 12=186(BTech(Hon)); 174+20= 194(BTech- MS) MMS)											
Semester –IX						**Semester -X**					
Course	**Course Name**	**L**	**T**	**P**	**C**	**Course**	**Course Name**	**L**	**T**	**P**	**C**
ICB XXX	Research Project	12	0	0	12	ICB XXX	Research Project	12	0	0	12
Total		**12**	**0**	**0**	**12**	**Total**		**12**	**0**	**0**	**12**
Cumulative Credits at the End of Fifth Year: 218(BTech-MS)											

Remark: *To meet the minimum requirement of 186 credits for qualifying the BTech (Hon)Degree, students may take two additional projects of 6 credits each and, to meet the requirement of 218 credits for BTech-MS, students may take two additional projects of 6 credits each, two 4 credit research courses and 24 credit research project in addition to 174 credits requirement of BTech Degree.*

B.TECH./B.TECH (HON)/DUAL DEGREE (B. TECH - MS) PROGRAMME

Sl No	Course Description	Minimum Credits Requirement			Period
		BTech	BTech (Hon)	BTech-MS	
1	Institute Core courses	94	94	94	Semester I to IV
2	Bouquet Core Courses	24	24	24	Semester V to VIII
3	Stream Electives	18	18	18	Semester V to VIII
4	Institute Open Electives	9	9	9	Semester V to VIII
5	Humanities Electives	3	3	3	Semester V to VIII
6	Science Electives	3	3	3	Semester V to VIII
7	Maths Electives	3	3	3	Semester V to VIII
8	Engineering Elective	4	4	4	Semester V to VIII
9	Any other elective/Industrial Training	4	4	4	Semester V to VIII
10	BTech Projects	12	12	12	Semester VII to VIII
11	Honours Project		12	12	Semester VI to VIII
12	Research Courses			8	Semester VII to VIII
13	Research Project			24	Semester IX to X
Total Credits required for Successful Completion		**174**	**186**	**218**	
Minimum CGPA required for Successful Completion		**5.5**	**8.0**	**8.0**	

SEMESTER I

IMA 111 Discrete Mathematics [3-1-0-4]

Objectives of the course

- To extend student's Logical and Mathematical maturity and ability to deal with abstraction
- To introduce most of the basic terminologies used in computer science courses
- To explain and apply the basic methods of discrete mathematics in Computer Science.
- To able to write clear, concise and correct mathematics proofs.
- To solve counting problems involving permutations and combinations and apply Pigeon hole principle
- To understand the basics of graph theory and group theory

Outcomes of the course

- Have knowledge of the concepts needed to test the logic of a program.
- Have an understanding in identifying structures on many levels.
- Be aware of a class of functions which transform a finite set into another finite set which relates to input and output functions in computer science.
- Be able to apply basic counting techniques to solve combinatorial problems
- Acquire ability to describe computer programs in a formal mathematical manner.

Syllabus

Logic: Propositions, negation, disjunction and conjunction, implication and equivalence, truth tables, predicates, quantifiers, rules of inference, methods of proof.

Set theory: definition and simple proofs in set theory, Inductive definition of sets and proof by induction, inclusion and exclusion principle, relations, representation of relations by graphs, properties of relations, equivalence relations and partitions, partial orderings, linear and well-ordered sets.

Functions: mappings, injection and surjections, composition of function, inverse functions, special functions, recursive function theory.

Elementary combinatorics: Counting techniques, pigeonhole principle, recurrence relation, generating functions.

Graph theory: Elements of graph theory, Euler graph, Hamiltonian path, trees, tree traversals, spanning trees.

Algebra: groups, Lagrange's theorem, homomorphism theorem, rings and fields, structure of the ring Zn and the unit group Zn*, lattice

Textbooks/References

1. Kenneth H. Rosen, Discrete Mathematics and Its Applications, Seventh Edition, Mcgraw-Hill, 2017.
2. Norman L. Biggs, Discrete Mathematics, Oxford University Press, Second Edition, 2003.
3. J.P. Tremblay, R. Manohar, Discrete Mathematical Structures with applications to Computer Science, McGraw Hill,2017.
4. K.A. Ross, C.R. B. Wright, Discrete Mathematics, 5th Edition, Pearson, 2003.
5. P. B. Bhattacharya, S. K. Jain, S, R. Nagpaul, Basic Abstract Algebra, Second Edition, Cambridge University Press, 2003.
6. J.A. Gallian, Contemporary Abstract Algebra, Ninth Edition, Cengage Learning, 2017.

ICS 111 IT Workshop I [3-1-3-5]

Course Objectives

To extend student's knowledge in basics of computers and networks. This enables students to understand the internals of systems, which includes hardware parts, software and its installation procedure, basic Linux commands. Students would also be getting familiar with various networking terminologies and its components. They would be also studying to setup and develop a dynamic web application.

Course Outcomes:

- Have a knowledge of the various hardware components.
- Have an understanding of Linux commands and shell scripting.
- Be aware of basic networking concepts, devices and its functionality.
- Be aware of the basic web development scripting languages like HTML, CSS, XML, and JavaScript.

Syllabus

Computer Hardware – Prerequisite, Computing Agents CPU, Memory, Motherboard - Computer Peripherals - I/O devices, Storage devices, Interface cards – Buses – Firmware - Boot process - Writing/formatting media.

Computer System Software - Operating Systems, Unix/Linux commands, Shell scripting. Computer Communications – LAN, WAN, Client/Server networks, Peer-to-Peer networks, Topologies, Basics of TCP/IP, IP addresses, DNS, Routers, Internet, WWW, FTP, Email servers, Web servers.

Web Design - Basics of HTML, CSS, XML, and JavaScript.

Lab - Practice

Computer Hardware – Familiarization CPU Box, Mother board, CPU & Chip-set, Interface cards, Card slots, Hard disk, Cables, SMPS, NIC, Various ports, etc.

Computer Peripherals - I/O Devices. Storage devices, Interface cards – Buses – Firmware - Boot process - Writing/formatting media.

Computer System Software - Operating Systems, Windows, Linux, Commands

Unix/Linux commands, Shell scripting. Client/Server networks, Peer-to-Peer networks, LAN, WAN, MAN.

Familiarization of - Basics of TCP/IP, IP addresses, DNS, Routers, Internet, WWW, FTP, Email servers, Web servers.

Web Design - Basics of HTML, CSS, XML, Java Scripting

Text Books/References

1. G. Michael Schneider, Judith Gersting, Invitation to Computer Science, Seventh Edition, 2015.
2. Computer Science Illuminated, Jones & Bartlett Learning; Sixth Edition, 2016. Jennifer Niederst Robbins, Learning Web Design, O'Reilly Fourth Edition, 2012.
3. Ron White, How Computers Work: The Evolution of Technology, Que Publishing; Tenth Edition, 2014.
4. Alan Clements, Principles of Computer Hardware, Oxford University Press India, Fourth Edition, 2013.
5. David Reed,A Balanced Introduction to Computer Science, Pearson, Third Edition, 2010.
6. Peter Norton's Intro to Computers, Peter Norton, McGraw-Hill Higher Education, Sixth Edition, 2005.
7. Steven Holzner, PHP: The Complete Reference, McGraw Hill Education, 2017.
8. Arnold Robbins and Nelson H. F. Beebe, Classic Shell Scripting, O'Reilly Media, 2008.
9. Richard Peterson, Linux: The Complete Reference, McGraw Hill Education Sixth Edition, 2017

ICS 112 Computer Programming [3-1-3-5]

Course Objectives

To introduce the problem-solving processes/ techniques

- to teach computer programming
- to use C & C++ for solving the problems

Course Outcomes

Students learn how to write the sequence of operations in solving a problem

- Students learn to translate the problem-solving steps to a program
- Students learn the use of programming language for solving real world problems on a computer

Syllabus

Basics of computers: software/ systems, Programming- Introduction, Problem solving- Introduction, Problem solving techniques: definition of problems, solutions, top-down approach, breaking problem in to sub-problems.

Algorithms: - writing the steps required solving problems, representing algorithms as flow chart, translating to procedure/ functions. Modularity

Example problems: computation of factorial, sine, Mod arithmetic-computation of quotient/ remainder, solving factorial through recursion, etc. Object technology- introduction, C++ data types/ scope rules, C++ control statements, Example problems/ program, Example problems/ program, Character handling, Pointers, functions, Classes and objects, Classes and objects.

Lab Practice

Implement fundamental domain knowledge of the course for developing effective computing solutions by incorporating creativity and logical reasoning.

Students are encouraged to use the lab sessions as a multi-use, technology-enhanced teaching space with characteristics of both classrooms and labs.

Understand and learn how a big program can be broken up into independent modules and define functions and call them with appropriate parameters.

Students should gain a clear idea of how decision making and various basic/advanced constructs for control flow and instruction repetition is done while programming.

Students should learn how to use arrays for storing/retrieving large amount of data. They should also understand the concept of strings and string libraries used for their manipulation.

Comprehend how to use structures as a compound datatype. Students should also acquire the capability to design structures according to their requirement.

Understand recursion, pointer referencing/dereferencing and dynamic allocation of memory.

Text Book/References

1. R G Dromey, How to Solve It by Computer, Prentice-Hall International Series in Computer Science, 2006.
2. G.Michael Schneider, Invitation to Computer Science, Eighth Edition, 2018.
3. Byron S Gotrified, Programming with C, Thrid Edition, McGraw Hill Companies, 2017.
4. Michael Vine, C Programming for the Absolute Beginner, Third Edition, 2014.
5. Brian W Kernighan, Dennis M. Ritchie, C Programming Language, Second Edition, Pearson Education India, 2015.
6. Herbert Schildt, C++ Complete Reference, McGraw Hill, Fourth Edition, 2017.
7. Eric Nagler, Learning C++: A hands-on Approach, Third Edition, Cengage learning, 2017.

IEC 111 Electronic Circuits and Measurements [3-1-3-5]

Course Objectives

- To impart the basic concepts of semiconductor devices
- To make students capable of analyzing the operation of various electronic circuits
- To develop knowledge for designing simple analog circuits using discrete and integrated components.
- To familiarize the students with the construction and working principle of different types of sensors and transducers.
- To give awareness about the measuring instruments and the methods of measurement.

Course Outcomes:

- Characterize semiconductor devices like diodes, transistors, FETs and operational amplifiers.
- Apply the knowledge of semiconductor devices to Design and implement basic electronic circuits.
- Use concepts in common use for converting a physical parameter into an electrical quantity.
- Choose proper sensor comparing different standards and guidelines to make sensitive measurements of physical parameters like temperature, pressure, flow, acceleration, etc.

Syllabus

Diodes: Introduction to diodes, Semiconductor materials, Diode Characteristics, Operation, Diode Applications, Rectifiers, Clipping and Clamping Circuits, Zener Diodes as regulators

Bipolar Junction Transistors (BJTs): Introduction to transistors, Transistor Construction, Operation, NPN and PNP transistors, Transistor Voltages and Currents, Transistor Characteristics. Common base and Common emitter transistor configurations, Biasing BJTs: Fixed bias, Emitter-Bias, Voltage Divider Bias, Emitter Follower bias , Collector Feedback bias, Transistor Amplification, Transistor as a switch

Field Effect Transistors: Introduction, JFET, MOSFET, Characteristics, Depletion Type,

Enhancement type, FET Biasing, Different configurations, Amplification, FET as a switch.

Operational Amplifier (Op-amp): Introduction, Differential amplifier, Ideal Op-amps, parameters, Op-

amp Applications: voltage Adder, Subtractor, Integrator, Differentiator circuits, constant gain multiplier, voltage buffer.

Principles of sensing & transduction, Introduction to Mechanical and Electromechanical sensors, Strain gauge, Inductive sensors, Capacitive sensors, Thermal sensors, Magnetic sensors, Smart Sensors.

Lab Practice

Familiarization of Basic Electronic Lab Equipments, Familiarization of Diodes, Testing. Diode characteristics, Diode Circuits: Rectifiers, Regulators, Clipping and Clamping Circuits.

Familiarization of Transistors, Bipolar Junction Transistor Testing, Characteristics, Biasing,

Amplifiers, Oscillators.

Junction Field Effect Transistor Familiarization, Testing, Characteristics, Biasing, Amplifiers.

Operational Amplifier (Op-amp) Familiarization, Testing, Op-amp circuits, amplifiers, detectors etc.

Text Books/References

1. David A Bell, Electronic Devices and Circuits, Oxford University Press, Fifth Edition, 2008.
2. Sedra A. and Smith K. C, Microelectronic Circuits", Oxford University Press, Sixth Edition, 2011.
3. Robert. L. Boylestad, Louis Nashelsky, Electronic Devices and Circuits Theory, Pearson Education, Eleventh Edition, 2015.
4. Jacob Millman and Christos. C. Halkias, Electronic Devices and Circuits, Mc. Graw Hill, Fourth Edition, 2015.
5. Albert Malvino and David J Bates, Electronic Principles, Seventh Edition, McGraw Hill, 2006.
6. S Franco, Design with Op-Amp and analog integrated circuits, Third Edition, McGraw Hill, 2001.
7. Sensor & transducers, D. Patranabis, 2nd edition, PHI
8. Instrument transducers, H.K.P. Neubert, Oxford University press.
9. Measurement systems: application & design, E.A.Doebelin, Mc Graw Hill.

IHS 111 Communication Skills [3-0-0-3]

Course Objectives

The objective of the class was to improve the English communication skills of First Semester B. Tech students who had just passed out of their Senior Secondary classes. This was challenging since the class included students from various parts of the country speaking various mother tongues.

The syllabus is designed to give importance to essential grammar, as well as reading, writing and speaking skills. Based on this, work in class consisted of teaching grammar, interspersed with written exercises, reading practice, reading comprehension, business letter writing, report writing, training in preparing CV for job applications, group discussion and ex tempore speaking. The classes were rounded off with some training in the so called "soft skills".

Course Outcomes

At the end of the sessions, improvement in English language ability was noted in most of the students. A large number showed very good improvement, while even the least competent registered some improvement. Under the circumstances, the objective of the class would appear to have been achieved.

Syllabus

Communication, verbal and non-verbal, Conversation: formal and informal, prepared and extempore, English: British/American/Indian, Vocabulary development: reading, use of dictionaries, Expression: writing, Pronunciation: phonetics, use of phonetic dictionaries, speaking, English grammar: Basics: Parts of speech: Noun, Pro-noun, Adjective, Verb, Adverb, Preposition, Conjunction, Interjection .Verb: Tenses. Sentence structure: S+V.Concord: Subject-Verb agreement.Reported speech,Active and passive voice, Tag questions, Confusing words and expressions,Synonyms and antonyms,Idioms and phrases, Common errors in English,Punctuation.Writing skills: Letters: Formal/Informal, Reports,CV. Comprehension: Listening/Reading/Making notes/ Summarising, Interview skills, Group discussion,Soft-skills.

Text Books/References

1. A.J. Thomson & A.V. Martinet.A Practical English Grammar. Delhi: OUP.
2.George Yule.xford Practice Grammar: Advanced.Oxford:OUP.
3.Raymond Murphy.Essential English Grammar. Delhi: Cambridge University Press.
4.Matthew Monippally.The Craft of Business Letter Writing. New Delhi: Tata McGraw-Hill.

IHS 112 Foreign Language [1-0-0-1]

Course Objectives

The primary objective of the course is to introduce the basics of French language and grammar to the students. This course helps the students to develop the four language skills at the initial level. It covers the fundamentals of French language, such as French alphabets and

phonetics, essential grammar and simple vocabulary. This course will also provide students with a fundamental understanding of the French language and culture. Students will have knowledge in several core competencies in areas like: listening, reading, speaking and writing.

Course Outcomes

Use French well enough to describe, narrate, and ask/answer questions in the present time about a variety of topics related to the family, daily activities, and the place you live. The students should also be able to express him/herself effectively and accurately in simple French about him/herself and his/her surroundings in the present tense, near future and in recent past tense. Students will be able to make short statements and ask/answer simple questions in the past. Comprehend French with sufficient ability to grasp the main idea and some supporting details in short conversations (spontaneous or recorded) that pertain to the topics mentioned above. Read and understand the main idea and some details of materials (both literary and nonliterary) about a variety of topics. Write sentences and short paragraphs on familiar topics relating to personal interests and practical needs. Begin to develop an awareness of French and francophone cultures. Begin to understand on a basic level how French functions as a language.

Syllabus

Salutations, Alphabets, Presentation (to introduce someone), Conjugation of First and Second group verbs, Interrogative sentence. Numbers from 0 to 100.

Definite and Indefinite articles, French vocabularies, French foods, Costumes etc., Conjugation of third group and irregular verbs, Negation, Prepositions of places, Possessive adjectives, The Family

About house,Activities and hobbies, Reflexive verbs, Pronom toniques,Conjunctions, Article contracté,Partitive, articles,Possessive form,Future Tense.

Simple prepositions and negation, Seasons,Adjectives,Irregular adjectives,Recent past,Demonstrative adjectives,Time

Text Books/References

1. Apprenons le français 1- Méthode the français 1 & Cahier d'exercices by Mahitha Ranjith & Monica singh
2. Saison 1- Méthode the français 1 & Cahier d'exercices- Didier
3. Écho A1- Méthode Version numérique- DVD- CLE International
4. La tendance- Conversation videos

SEMESTER II

IMA121 Calculus and Linear Algebra [3-1-0-4]

Course Objectives

- To Study the basic topological properties of the real numbers
- Have the knowledge of the sequence of real numbers and convergence.
- Studying the notion of continuous functions and their properties.
- To gain an understanding of the linear system of equations
- To get introduced to the fundamental concepts of vector spaces
- To impart the basics of linear transformation, orthogonalization, basis, dimensions and eigenvalues.
- To provide the knowledge to apply the concepts of linear algebra in engineering applications.

Course Outcomes

- Have a good knowledge of the mathematical concepts in real analysis
- Be able to prove statements and to formulate precise mathematical arguments.
- To solve the problems related to linear systems and matrices
- To apply the knowledge of linear transformation, orthogonal projections, ortho-normalization and Least-square solutions in engineering applications.

Syllabus

Calculus: The Natural Numbers,The Peano axioms; Real Numbers; Properties of Real Numbers; Least upper bound and greatest lower bound properties: Sequences and Series: Convergence and limit laws, Finite and infinite series, Sums of non-negative numbers, Absolute and conditional convergence of an infinite series, tests of convergence; Continuous function on R: left and right continuity, examples of continuous and discontinuous functions, The Maximum principle, Intermediate value theorem, Monotonic functions, Uniform continuity. Differentiation of functions: Definition and basic properties, Local maxima, local minima, and derivatives, Monotone functions and derivatives, , Rolle's theorem, Mean value theorem: The Riemann Integration: Upper and lower Riemann integrals, Basic properties of Riemann integral, Riemann integrability of continuous functions, monotone functions, and discontinuous functions, The fundamental theorems of calculus

Linear Algebra: Fields, System of linear equations, Matrices and elementary row operations, Row reduced echelon matrices, Matrix multiplication, Invertible matrices, Rank of a matrix. Definition of a linear vector space and examples; linear independence of vectors, basis and dimension, Subspaces; Linear transformations,

Isomorphism, Linear functionals, the double dual; Inner product, orthogonal basis, Gram-Schmidt orthogonalization process; linear operators; Orthogonal and Hermitian matrices, Eigen vectors of a matrix and matrix diagonalization, Applications.

Text Books/References

1. R. G. Bartle and D. R. Sherbert, Introduction to Real Analysis, Fourth Edition, Wiley, 2011.
2. T. M. Apostol, Calculus, Volume I, Second Edition, Wiley, 2007.
3. Gilbert Strang, Linear Algebra and Its Applications, 5 edition, Wellesley-Cambridge Press/Siam, 2016
4. K. Hoffman and R. Kunze, Linear Algebra, 2 edition, PHI, 2009
5. Erwin Kreyzig, Advanced Engineering Mathematics, Tenth Edition, Wiley, 2015.

IEC 121 Digital Design and Electric Circuits [3-1-3-5]

Course Objectives

The primary objective of this course is to provide the student with the fundamental concepts and skills necessary to analyze and design combinational and sequential logic circuits. The course explains the basics of analog and digital logic circuits. It also introduces the student a hardware description language and its application to the design of combinational, sequential and simple digital systems. The material covered in the lecture is reinforced through practical experience in the associated lab together with the use of Verilog HDL to synthesize logic circuits.

Course Outcomes

- Understand the fundamentals of analog and digital circuits.

- Analyze and design a circuit of logic gates that have the desired relation between the input and output terminals.
- Understand the logic properties of flip flops .
- Analyze and design counters, registers, and similar circuits.
- Implement combinational and sequential circuits using a hardware description language.

Syllabus

Introduction - Analog and Digital circuits – Kirchhoff's Laws, Superposition Theorem, Thevenin's and Norton's Theorems; Review of Number Systems - Number systems and conversions-decimal, binary, 1's and 2's complements, hexadecimal, octal etc. Logic gates-NOT, AND, OR, XOR, XNOR, Universal gates, timing diagrams.

Boolean algebra-DeMorgans theorems, SOP and POS forms. Karnaugh Maps-to simplify Boolean expressions, truth table functions. Combinational Logic-Analyze basic combinational logic circuits, design a combinational logic circuits for a given truth table. Functions of Combinational logic-comparators, adders, code converters, multiplexers, de-multiplexers.

Sequential Circuit Design - Flip-Flops and Latches. SR, D, and JK Flip-Flops. Edge-triggered and Master-Slave Flip-Flops, Excitation table. Counters – Design of asynchronous and synchronous counters. Timing diagrams up/down counters. Shift Registers – data movements in shift registers. SISO, SIPO, PISO, PIPO shift registers.

Memory and programmable logic – RAM, Memory decoding, ROM, PLA, PAL, sequential programmable devices, overview of logic design using Verilog HDL, Basic concepts, Modules, Ports.

Lab Practice

Familiarization of Logic Gates.

Design of Combinational Logic Circuits – Comparators, Adders, Code Converters, Multiplexers, Demultiplexers etc.

Familiarization of Flip-Flops and Latches. SR, D, and JK Flip-Flops. Edge- triggered and Master-Slave Flip-Flops.

Design of Sequential Logic Circuits, Design of Counters, Asynchronous Counters, Synchronous counters. Shift Registers.

Simple Verilog HDL programs.

Text Books/References

1. Floyd, Digital Fundamentals, McGraw Hill, Tenth Edition, 2011.
2. Morris Mano, Digital Circuits and Logic Design", PHI Publication, Fifth Edition, 2015.

ICS 121 Data Structures I [3-1-3-5]

Course Objectives

- Define and describe simple data structures like arrays, linked lists, trees and graphs
- Design and specify algorithms for searching and sorting, and those associated with the above data structures
- Analyze simple algorithms, like sorting and searching using mathematical tools, like formulation and solving of recurrences, asymptotic analysis and probabilistic analysis
- Analyze application problems and abstract them to formulate solutions involving data structures and algorithms

Course Outcomes

- Students learn to define operations of data structures like arrays, linked lists, trees and graphs
- Students learn to design and specify algorithms involving above types of data structures
- Students learn to analyze simple algorithms and solve recurrences, asymptotic analysis and probabilistic analysis
- Students learn to analyze application problems and abstract them to formulate solutions involving data structures and algorithms

Syllabus

Introduction- Algorithm Analysis, Finding Complexity. Fundamental data structures - List- Sorted Lists, Double Linked Lists, Skip list
Stack & Queue application.- Celebrity problem, histogram rectangular area problem

Binary Trees – Insertion and Deletion of nodes, Tree Traversals, Polish Notations, Red Black Trees, B-Trees, Heaps, Priority Queues.

Optimal binary search tree, Application problems on Optimal binary search Tree

Sorting – Bubble, Selection, Insertion, Merge Sort, Quick Sort, Radix Sort, Heap sort. Searching.

Hashing- Application problems on hashing

Graphs- Shortest path algorithms, Minimum Spanning Trees, BFS, DFS.

Text Books/References

1. Clifford A Shaffer, Data Structures and Algorithm Analysis, Edition 3.2 (Java Version), 2011.
2. Michael T. Goodrich, Roberto Tamassia, Michael H. Goldwasser. Data Structures And Algorithms In Java™ Sixth Edition, Wiley Publishers, 2014.
3. Mark Allen Weiss Data Structures And Algorithm Analysis In Java, Third Edition, 2012.
4. Robert L. Kruse, Data Structures And Program Design In C++, Pearson Education, Second Edition, 2006.
5. Ellis Horowitz, Fundamentals of Data Structures in C++, University Press, 2015.
6. Ajay Agarwal, Data Structure through C, A Complete Reference Guide, Cyber Tech Publications, 2005.

ICS122 Computer Organization [3-1-0-4]

Course Objectives

- To understand the basics of computer hardware and how software interacts with computer hardware.
- To analyze and evaluate the performance of computers.
- Understand basics of Instruction Set Architecture (ISA) – RISC.
- To understand how computers represent and manipulate data.
- To understand how computer perform arithmetic operations, how they are optimized and made to run faster.
- To understand how the memory management takes place in a computer system.
- To understand what is pipelining, and the design concepts involved.

Design a simple computer with hardware design including data format, instruction format, instruction set, addressing modes, bus structure, input/output, memory, Arithmetic/Logic unit, control unit, and data, instruction and address flow.

Course Outcomes

- This course will introduce to students the fundamental concepts underlying modern computer organization and architecture.
- Students should be able to know the overall working of a computer.
- Students should be able to get a detailed understanding of the design principles involved in developing a computer.
- They should know the representation of data, how programs are represented, executed and how programs manipulate and operate on data.
- They should also be able to appreciate how the memory organization is done and how to organize memory for faster execution of programs.
- Students should also be able to appreciate the concepts in pipelining.

Syllabus

Computer abstraction and technology: Basic principles, hardware components, Measuring performance: evaluating, comparing and summarizing performance. Instructions: operations and operands of the computer hardware, representing instructions, making decision, supporting procedures, character manipulation, styles of addressing, starting a program.

Computer Arithmetic: signed and unsigned numbers, addition and subtraction, logical operations, constructing an ALU, multiplication and division, floating point representation and arithmetic, Parallelism and computer arithmetic.

The processor: building a data path, simple and multi-cycle implementations, microprogramming, exceptions, Pipelining, pipeline Data path and Control, Hazards in pipelined processors

Memory hierarchy: caches, cache performance, virtual memory, common framework for memory hierarchies Input/output: I/O performance measures, types and characteristics of I/O devices, buses, interfaces in I/O devices, design of an I/O system, parallelism and I/O. Introduction to multicores and multiprocessors.

Text Books/References

1. D. A. Pattersen and J. L. Hennesy, Computer Organisation and Design: The Hardware/ Software Interface, Fourth Edition, Morgan Kaufman, 2009.
2. V. P. Heuring and H. F. Jordan, Computer

System Design and Architecture, Prentice Hall, 2003.
3. J. L. Hennessy and D. A. Patterson, Computer Architecture: A Quantitative Approach, Fifth Edition, Morgan Kaufman, 2011.
4. Carl Hamazher, ZvonkoVranesic and SafwatZaky, Computer Organization, Fifth Edition, McGraw Hill, 2002.

ICS 123 IT Workshop II [2-1-3-4]

Course Objectives

To introduce the object-oriented problem-solving processes/ techniques

- To learn Object oriented programming
- To use JAVA application development platforms and Android application development platform

Course Outcomes:

- Students learn OOP development on Eclipse and developer platform
- Students learn GUI based programming
- Students learn to develop android and mobile applications
- Students learns to write larger complex applications

Syllabus

Introduction to OOPs and Java Language Fundamentals - OOPs Principles, Features of Java. JVM, Bytecode, JRE, Language Fundamentals.

Classes and Objects- Introducing class fundamentals, Object and Object reference, Introducing methods, Extending Objects, Object Life time & Garbage Collection, Creating and Operating Objects, Constructor & initialization code block, Access Control, Modifiers, Nested, Inner Class and Anonymous Classes, Abstract Class and Interfaces, Defining Methods, Argument Passing Mechanism, Method Overloading, Recursion, Dealing with Static Members, finalize() method, native Method. Use of "this " reference, Use of Modifiers with Classes & Methods, Method overriding, Package and Interfaces, Garbage Collection.

Extending Classes and Inheritance Use and Benefits of Inheritance in OOP, Types of Inheritance in Java, Role of Constructors in inheritance, Overriding Super Class Methods, use of "super", Polymorphism in inheritance, Implementing interfaces.

Package Organizing Classes and Interfaces in Packages, Package as Access Protection.

Exception Handling: Exceptions & Errors, Types of Exception, Control Flow in Exceptions.

Array & Strings: Defining an Array, Initializing & Accessing Array, Multi –Dimensional Array, Operation on String, Mutable & Immutable String, Using Collection Bases Loop for String, Tokenizing a String, Creating Strings using String Buffer

Application problems on Linked list, stack in Java, Priority Queue in Java using comparators, hashmap

Introduction to PHP app development- Introduction to PHP, Basic Syntax of PHP, PHP statement terminator and case insensitivity, Embedding PHP in HTML, Comments, Variables, Assigning value to a variable, Constants, Managing Variables; Operators and Controls Structures; Functions in PHP, Arrays, PHP File and Forms Handling- File Open, File Creation, Writing to files, Reading from File, Searching a record from a file, Closing a File, PHP Server-side programming - Using PHP With HTML Forms, GET and POST methods, Sessions and Cookies, Support for Database, Creating classes in PHP.

Text Books/References

1. C. Thomas Wu, An Introduction to Object Oriented Programming with Java, Fifth Edition, 2009.
2. Ken Arnold, James Gosling and David Holmes, The Java Programming Language, Fourth Edition, 2005.
3. Herbert Schildt, Java: The Complete Reference, McGraw Hill Education(India), 11th Edition 2018.
4. Steven Holzner, PHP: The Complete Reference, McGraw Hill Education, 2017.

IHS 121 Personality Development [1-0-0-1]

Course Objectives

- To understand the basic perspectives of human personality such as; Trait approach, Psychoanalytic approach, Biological basis, Humanistic/phenomenological approach, Behaviorist/learning, Cognitive approach , Interaction perspective, and Transpersonal perspective (Indian and Yoga Psychology).

- Learn to objectively assess and explain the behavior of other people, identify personality traits so as predict how a person will behave, and to help to function effectively.

Course Outcomes

- Have understanding how hiring decisions are taken based on personality characteristics that serve as requirements of a job
- Understanding the application of assessment of Type A & B personality on personal health & achievement
- Understand Personality disorders and its identification. Cognitive Behavior Therapy in the context of Psychotherapy for personality disorders.

Syllabus

Understanding one's own personality and that of others, appreciate uniqueness of individuals, adapt to people and situations effectively, assess self and others using scientific tools of personality, cope with challenges in life with better understanding of human behavior science. Personality: Meaning & Assessment. Psychoanalytic & Neo-Psychoanalytic Approach ; Behavioural Approach; Cognitive Approach; Social- Cognitive Approach; Humanistic Approach; The Traits Approach; Models of healthy personality: the notion of the mature person, the self-actualizing personality etc. Personality disorders; Psychotherapeutic techniques and Yoga & Meditation; Indian perspective on personality; Personality in Socio-cultural context.

Text Books/References

1. Schultz, D.P., & Schultz, S. E. (2005)(8th Edn.)Theories of Personality. Belmont: Thomson Wadsworth.
2. Lindzey, G., Campbell, J.B., & Hall, C.S.(2007)(4th Edn.). Theories of Personality. NewYork:Wiley & Sons
3. Ryckman, R.M. (2008)(9th Edn.).Theories of Personality.Belmont: Thomson Wadsworth.
4. Rao, K.R., & Paranjpe, A.C.(2016).Psychology in the Indian Tradition. NewDelhi:Springer.
5. Frankl, V.E.(1992). Man's Search for Meaning. Massachusetts:Beacon Press
6. Simanowitz, V., & Pearce, P. (2003). Personality Development.England: Open University Press.

SEMESTER III

IMA 211 Probability, Statistics and Random Processes [3-1-0-4]

Course Objectives

- To expose the students to the modern theory of probability, concept of random variables and their expectations.
- To introduce various discrete and continuous distributions and concept of estimation theory, confidence interval.
- To illustrate the concept of hypothesis testing, tests for means and variances, Goodness of fit tests
- To introduce the concept of random processes, Markov chains, Brownian Motion.

Course Outcomes

- Define and apply the concepts of probability and conditional probability
- Define and illustrate discrete and continuous random variables, their probability mass functions and probability density functions
- Understand the concept and need of hypothesis testing
- Perform the tests for means and variances and Goodness of fit test
- Understand the concept of random processes, Markov chains, Brownian motions.

Syllabus

Axiomatic construction of the theory of probability, independence, conditional probability, and basic formulae.

Random variables and distributions: Univariate, Bivariate and multivariate random variables, Cumulative and marginal distribution function, Conditional and multivariate distributions, Functions of random variables: Sum, product, ratio, change of variables.

Mathematical expectations, moments, moment generating function, characteristic functions; Discrete/continuous distributions and limit theorems: Binomial distribution, Geometric distribution, Poisson distribution, Normal distribution, Exponential distribution, Gamma distribution, Beta distribution, Central limit theorem, Tchebeyche's inequality, Law of large numbers

Estimation Theory: Bias of estimates, Confidence intervals, Minimum variance unbiased estimation, Bayes' estimators, Moment estimators, Maximum likelihood estimators, Chi-square distribution, Confidence intervals for parameters of normal distribution

Hypothesis testing: Tests for means and variances, hypothesis testing and confidence intervals, Bayes' decision rules, Power of tests, Goodness-of-fit tests, Kolmogorov-Smirnov Goodness-of-fit test

Definition and classification of random processes, discrete-time Markov chains, Poisson process, continuous-time Markov chains, stationary processes, Gaussian process, Brownian motion

Text Books/ References

1. S. Ross, Introduction to Probability and Statistics for and Engineers and Scientists, Third Edition, Elsevier, 2004.
2. P. G. Hoel, S. C. Port and C. J. Stone, Introduction to Probability Theory, Universal Book Stall, 2000.
3. S. M. Ross, Introductory Statistics, Second Edition, Academic Press, 2009.
4. J. Medhi, Stochastic Processes, Third Edition, New Age International, 2009.
5. V.K.Rohati and A.K. Saleh, An introduction to Probability and Statistics, Third Edition. Wiley Student Edition, 2006.
6. G. R. Grimmett and D. R. Stirzaker, Probability and Random Processes, Oxford University Press, 2001.
7. W. Feller, An Introduction to Probability Theory and its Applications, Vol. 1, Third Edition.,Wiley, 1968.
8. S.M. Ross, Stochastic Processes, Second Edition. Wiley, 1996.
9. C. M. Grinstead and J. L. Snell, Introduction to Probability, Second Edition, Universities Press India, 2009.
10. S.Ross, A First Course in Probability, 10th Edition, Pearson Education, Delhi, 2018.

ICS 211 Design and Analysis of Algorithms [3-1-0-4]

Course Objectives

- Analyze the asymptotic performance of algorithms.
- Demonstrate a familiarity with major algorithms and data structures.
- Apply important algorithmic design paradigms and methods of analysis

- Synthesize efficient algorithms in common engineering design situations.

Course Outcomes

- Argue the correctness of algorithms using inductive proofs and invariants.
- Analyze worst-case running times of algorithms using asymptotic analysis.
- Describe the divide-and-conquer paradigm and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize divide-and-conquer algorithms. Derive and solve recurrences describing the performance of divide-and-conquer algorithms.
- Describe the dynamic-programming paradigm and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize dynamic programming algorithms, and analyze them.
- Describe the greedy paradigm and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize greedy algorithms, and analyze them.
- Explain the major graph algorithms and their analyses. Employ graphs to model engineering problems, when appropriate. Synthesize new graph algorithms and algorithms that employ graph computations as key components, and analyze them.
- Explain what an approximation algorithm is, and the benefit of using approximation algorithms.

Syllabus

Introduction: Efficiency – Run Time & Space. Analyzing an Algorithm – Insertion Sort- Proof of Correctness – Complexity – Asymptotic Notations

Divide and Conquer: Analyzing Recursive Algorithms – Merge Sort, Recurrence Relations – Binary Search. Solving Divide and Conquer Recurrences – Recursion Tree – Substitution Method – Master Theorem – Applications of the Master Theorem.

Greedy Algorithms: Locally Optimal Solutions – Interval Scheduling – Minimum Spanning Trees

Prim's Algorithm – Locally Modifying Solutions to Build Better Solutions – Exchange Arguments

Dijkstra's Algorithm – Kruskal's Algorithm – Knapsack – Huffman Coding

Dynamic Programming: Reusing work across sub computations – Definition of Dynamic Programming – Optimal Rod Cut Problem - Optimal Matrix Chain Multiplication - Bellman-Ford Algorithm, Floyd-Warshall Algorithm – Longest Common Subsequence – Machine Scheduling Problem. Application problems- Max Flow problems in flow networks.

Amortized Complexity Analysis – Aggregate Method, Accounting Method, Potential Method, Dynamic Tables – Balanced Trees

Intractable Problems: Polynomial Time – class P – Polynomial Time Verifiable Algorithms – class NP – NP completeness and reducibility – NP Hard Problems – NP completeness proofs – Approximation Algorithms

Text Books/References

1. Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, Clifford Stein - Introduction to Algorithms, MIT Press, Third Edition, 2010.
2. Jon Kleinberg, Eva Tardos, Algorithm Design ,Pearson Addison, Wesley, 2013.

ICS 212 Operating Systems [3-1-0-4]

Course Objectives

- To introduce the Fundamental concept of OS, and how OS works;
- To study the Building blocks of OS, Components of OS

Course Outcomes:

- Students will be able to design an OS,
- Students will be able to implement various components of OS,
- Students will be able to implement a small OS

Syllabus

Operating system overview: Computer System Organization, Operating System structure, operations of OS, process management, memory management, storage management, protection and security, distributed systems.

Processes: Process concept, Process scheduling, Operations on processes, Cooperating processes, inter-process communication

Threads: Overview, Multi-threading models, threading issues, P threads, Windows XP threads

CPU Scheduling: Basic concepts, scheduling criteria, scheduling algorithms, multiple-processor scheduling

Process synchronization: The critical section problem, Peterson's solution, synchronization hardware, Semaphores, Monitors. Synchronization examples

Deadlocks: Methods for handling deadlocks, Deadlock prevention, deadlock avoidance, Deadlock recovery

Memory management: Swapping, Paging, Segmentation, Virtual memory, Demand paging, Page replacement

I/O Systems: I/O hardware, Application I/O interface, Kernel I/O subsystem, transforming I/O requests to hardware operations

Text Books/References

1. William Stallings, Operating systems: Internals & design principles, Pearson, Seventh edition, 2014.
2. Andrew S. Tanenbaum, Modern Operating Systems, Pearson Fourth Edition, 2016.
3. Charles Crowley, Operating Systems - Design Oriented Approach, Mc. Graw Hill Education, First edition, 2017.
4. Abraham Silberschatz, Galvin, Gagne Operating System Concepts, Wiley, Ninth Edition, 2016.

ICS 213 Database Management System [2-1-3-4]

Course Objectives

- To understand the need for a database and its management using DBMS
- To model Entity-Relationship (ER) diagram for a real-world scenario
- To write relational algebra and relational calculus queries for data handling and retrieval, Write SQL queries for database creation and analysis
- Design efficient database systems using the principle of normalization
- Understand the basics of database transactions, deadlock handling and security.
- How to implement database indexing
- Usage of tools like RA Interpreter and MySQL for executing various queries

Course Outcomes:

- Understand database concepts and structures and query language
- Understand the E R model and relational model
- Apply various Normalization techniques
- Understand query processing and techniques involved in query optimization.

Syllabus

Database Modeling: Database System concepts and architecture, Data modeling using Entity Relationship (ER) model and Enhanced ER model, Specialization, Generalization.

Database Indexing: Data Storage and indexing-Single level and multi-level indexing, Dynamic Multi level indexing using B Trees and B+ Trees

Relational Databases: The Relational Model, Relational database design using ER to relational mapping Relational algebra, Relational calculus, Tuple Relational Calculus, Domain Relational Calculus, SQL

Database Design: Database design theory and methodology, Functional dependencies and normalization of relations, Normal Forms, Properties of relational decomposition, Algorithms for relational database schema design

Database Transactions: Transaction processing concepts, Schedules and serializability, Concurrency control, Two Phase Locking Techniques, Optimistic Concurrency Control, Database recovery concepts and techniques

Database Security: Introduction to database security

Text Books/References

1. Ramez Elmasri and Shamkant B. Navathe, Fundamentals of Database Systems, Fifth Edition, Pearson Education, 2008.
2. Raghu Ramakrishnan and Johannes Gehrke, Database Management Systems, Third Edition, McGraw Hill, 2014.
3. Peter Rob and Carlos Coronel, Database System- Design, Implementation and Management, Seventh Edition, Cengage Learning, 2007.

ICS 214 IT Workshop III [2-1-3-4]

Course Objectives

- Learn Python scripting and the scripting shell.
- Master the basics of programming constructs, like conditions, loops, functions, etc.

- Introduce sequence types in Python like Lists, Tuples, Sets and Dictionaries
- Be exposed to advanced applications such as databases, networks, etc

Course Outcomes

- Write python programs for various applications
- Write Database programs to create, access, modify and update data
- Write network programs for sending emails, ftp, sockets etc

Syllabus

Introduction to data types, variables, constants, operators, input-output, basic formatting, running python programs, date and time functions

Conditionals, if statement and variants, relational operators, logical operators

Iteration and while loops, for loops and range command, random numbers

File processing, reading and writing files, parsing files, text files and CSV files

Lists and list processing, list operations, list traversals, tables as lists

Tuples, Maps, Sets and Dictionaries, creation and traversals

Strings and string processing, string functions, conversions

User defined Functions, lambda functions, recursive functions, built-in functions, yield statement, parameter passing

Classes and object-oriented programming, inheritance, associations

Database processing, creating tables, querying, MySQL and PySqlite

Network programming, sockets, email sending, ftp Threads and multithreading

Numpy and applications in matrices, random numbers Scipy, Matplotlib, graphing and charting data

Trie,stack, Networkx, pattern matching, regular expression

Introduction to Android app development.

Text Books/ References

1. Ljubomir Perkovic, Introduction to Computing with Python, Wiley, Second Edition, 2015.
2. Narasimha Karumanchi, Data Structures and Algorithms With Python, Careermonk Publications, 2015.

ISC 212 Quantum Computing and Security [2-0-0-2]

Prerequisite for the Course

Student should have a passing grade in, Discrete Mathematics (IMA 111) and Calculus and Linear Algebra (IMA 121) or the instructor's approval.

Course Objectives

1. To understand the principle of Quantum computing.
2. To design Quantum circuits and get hands-on experience using Qiskit.
3. To develop an efficient and secure Quantum cryptosystem.
4. To understand Quantum Cryptography and Quantum error correction.
5. To analyze quantum information security systems.

Course Outcomes

Students who successfully complete this course will be able to:-

1. Basic understanding about Quantum Information and Computation.
2. Design Quantum circuits in IBM quantum computers.
3. Understand the implication of Quantum Algorithms on classical Cryptosystems.
4. Understand the Quantum Cryptography and Quantum error correction.
5. Understand the Quantum Key Distribution and Secret Sharing protocols.

Syllabus

Introduction to Quantum Computing and Information: States, Operators, Measurements- Quantum search, Quantum Entanglement- Quantum Teleportation, Super-dense coding- Quantum gates and circuits.

Quantum Algorithms: Introduction, Deutsch–Jozsa algorithm, Grover's Algorithm,

Shor's Algorithm, and their cryptanalytic implications. Classical cryptography, Modern Cryptography, Quantum cryptography

Quantum error correction - The physics of error generation- Diagnosing error syndromes- Qbit error-correcting code

Quantum Security: Introduction, Quantum True Random Number Generators (QTRNG),

Quantum key distribution (QKD)

References

1. Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press, 2002.
2. A. O. Pittenger, An Introduction to Quantum Computing Algorithms (Birkhauser, 2000).
3. An Introduction to Quantum Computing, Phillip Kaye, Raymond Laflamme, and

Michele Mosca. Oxford U. Press, New York, 2007.
4. P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring.
5. Foundations of Computer Science (FOCS) 1994, page 124–134, IEEE Computer Society Press.
6. L. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of 28th Annual Symposium on the Theory of Computing (STOC), May 1996, pages 212–219. Available at http://xxx.lanl.gov/abs/quant-ph/9605043
7. Preskill Lecture notes. Available online: http://www.theory.caltech.edu/~preskill/ph229/.
8. Quantum Computer Science, N. David Mermin, Cambridge University Press 2007
9. https://csrc.nist.gov/projects/post-quantum-cryptography
10. B. S. Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley and Sons, New York, 1995.
11. A. Peres, Quantum Theory: Concepts and Methods, (Kluwer, 1993).
12. J. J. Sakurai, Modern Quantum Mechanics, 2d ed (Addison-Wesley, 2011).
13. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge, 2000).
14. G. Benenti, G. Casati, G. Strini, Principles of Quantum Computation and Information. Vol. 1: Basic Concepts, Vol II: Basic Tools and Special Topics (World Scientific 2004).
15. H.-K. Lo, T. Spiller, S. Popescu, Introduction to Quantum Computation and Information (World Scientific, 1998).
16. N. D. Mermin, Quantum Computer Science (Cambridge, 2007).

ICS 215 Data Structures II [1-0-3-2]

Course Objectives

- Teach programming with emphasis on problem solving and introduce Data structures.
- Provide the Foundations of the practical implementation and usage of Algorithms and Data Structures.

Course Outcomes:

- Design correct programs to solve problems.
- Choose efficient data structures and apply them to solve problems.

Syllabus

Problems on Geometric algorithms but not limited to: Klee's Algorithm, Manhattan distance problems, Collinear checking, Identifying Integral points inside a Triangle, Circumcenter of a Triangle, Triangular Matchstick Number, area of Circumcircle of an Equilateral Triangle, Number of rectangles in N*M grid, Area of two overlapping rectangles, Number of unique rectangles formed using N unit squares, Circle and Lattice Points, Pizza cut problem.

Algorithms on Bit Manipulation but not limited to: Letter manipulation problems, k-th bit Manipulation problems, Kernighan's Algorithm to count set bits in an integer.

Discussion on Numerical algorithms but not limited to: Gauss-Jordan Elimination, Matrix Manipulation problems.

Text Books/References

1. Cormen, Thomas H., et al. *Introduction to algorithms*. MIT press, 2009.
2. Aho, Albred V., J. E. Hopcroft, and J. D. Ullman. "*Data structures and algorithms* (1983).
3. Drozdek, Adam. *Data Structures and algorithms in C++*. Cengage Learning, 2012.
4. Allen, Weiss Mark. *Data structures and algorithm analysis in C++*. Pearson Education India, 2007.
5. Kleinberg, Jon, and Eva Tardos. *Algorithm design*. Pearson Education India, 2006.
6. Skiena, Steven S. *The algorithm design manual*. Springer International Publishing, 2020.
7. Knuth, Donald Ervin. *The art of computer programming*. Vol. 3. Pearson Education, 1997.
8. Nomura, Seiichi. "C Programming and Numerical Analysis: An Introduction." *Synthesis Lectures on Mechanical Engineering* 2.2 (2018): 1-198.
9. Dasgupta, Sanjoy, C. H. Papadimitriou, and U. V. Vazirani. "*Algorithms*; 2006."
10. Trefethen, Lloyd N., and David Bau III. Numerical linear algebra. Vol. 50. Siam, 1997.

SEMESTER IV

ICS 221 Theory of Computation [3-1-0-4]

Course Objectives

- Course will provide a formal connection between algorithmic problem solving and the theory of languages and automata and develop them into a mathematical (and less magical) view towards algorithmic design and in general computation itself.
- The course should in addition clarify the practical view towards the applications of these ideas in the engineering part of CS.

Course Outcomes:

- Model, compare and analyse different computational models using combinatorial methods.
- Apply rigorously formal mathematical methods to prove properties of languages, grammars and automata.
- Construct algorithms for different problems and argue formally about correctness on different restricted machine models of computation.
- Identify limitations of some computational models and possible methods of proving them.
- Have an overview of how the theoretical study in this course is applicable to and engineering application like designing the compilers.

Syllabus

Introduction: Notion of formal language- Strings, Alphabet, Language, Operations, Finite State Machine, definitions, finite automaton model, acceptance of strings and languages, deterministic finite automaton, equivalence between NFA and DFA, Conversion of NFA into DFA, minimization of FSM ,equivalence between two FSM's, Moore and Mealy machines.

Regular expressions: Regular sets, regular expressions, identity rules, manipulation of regular expressions, equivalence between RE and FA, inter conversion, Pumping lemma, Closure properties of regular sets regular grammars, right linear and left linear grammars equivalence between regular linear grammar and FA, inter conversion between RE and RG.

Context free grammars: Derivation, parse trees. Language generated by a CFG. Eliminating useless symbols, -productions, and unit productions. Chomsky Normal Form. Pushdown automata: Definition, instantaneous description as a snapshot of PDA computation, notion of acceptance for PDAs.

Turing machine: Turing machine, definition, model, design of TM, Computable Functions, recursive enumerable language, Church's Hypothesis, Counter machine, types of TM's, RAM machine

Un-decidability and classes of problems: Chomsky hierarchy of languages, linear bounded automata and context sensitive language, Grammar, decidability of problems, Universal Turing Machine, un-decidability of post's correspondence problem. Turing reducibility logical theories Complexity classes: P, NP, co-NP, EXP, PSPACE, L, NL, ATIME, BPP, RP, ZPP, IP.

Text Books/ References

1. M Sipser, Introduction to the Theory of Computation, Second Edition, Thomson, 2005.
2. Lewis H.P. and Papadimition C.H. Elements of Theory of Computation, Prentice Hall of India, Fourth Edition, 2007.
3. S. Arora and B. Barak, Computational Complexity: A Modern Approach, Cambridge University Press, 2009.
4. C. H. Papadimitriou, Computational Complexity, Addison-Wesley Publishing Company, 1994.
5. D. C. Kozen, Theory of Computation, Springer, 2006.
6. D. S. Garey and G. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, Freeman, New York, 1979.
7. J Hopcroft, JD Ullman and R Motwani, Introduction to Automata Theory, Languages and Computation, Third Edition, Pearson, 2008.

ICS 226 Secure Software Engineering [3-0-3-4]

Course Objectives

- Foundation on software engineering.
- Design and implementation of secure software.
- Introduce the role of security in the development lifecycle.
- To learn methodological approaches to improving software security during different phases of software development lifecycle.

- To know best security programming practices.

Course Outcomes:

- Understand the basics of software engineering.
- Explain terms used in secured software development and life cycle process.
- Incorporate requirements into secured software development process and test software for security vulnerability.
- Identify vulnerable code in implemented software and describe attack consequences.
- Apply mitigation and implementation practices to construct attack resistant software.
- Apply secure design principles for developing attack resistant software.

Syllabus

Introduction to software engineering: Scope and necessity; Software life cycle model: Waterfall model-Iterative waterfall model-Prototyping model-Evolutionary model-Spiral model-Agile development methodologies.

Requirement analysis and specification; System Design; Basic concepts in user interface design; Software testing; Software Project Management.

Security a software Issue: Introduction, the problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of Detecting Software Security.

Requirements Engineering for secure software: Introduction, the SQUARE process Model, Requirements elicitation and prioritization.

Secure Software Architecture and Design: Introduction, software security practices for architecture and design.

Security and Complexity; Governance and Managing for More Secure Software.

Textbooks/ Reference

1. Roger S Pressman, Software Engineering: A Practitioner's Approach, McGraw-Hill Higher Education, 7th Edition.
2. Ian Sommerville, Software Engineering, Pearson Education, 9th Edition.
3. Software Security Engineering: Julia H. Allen, Pearson Education
4. Developing Secure Software: Jason Grembi, Cengage Learning
5. Software Security: Richard Sinn, Cengage Learning

ICS 223 Compiler Design [3-0-3-4]

Course Objectives

- The main outcome of the course 'Compiler Design' is to make the students capable of applying the principles, algorithm, and data structures involved in the design of compilers.
- Students should be able to design a lexical analyser in lex according to the specification. They should be able to design a parser in yacc when the specification is mentioned. They should be able to construct a compiler according to the rules and constrains given.

Course Outcomes

- To introduce the major concept areas of language translation and compiler design.
- To enrich the knowledge in various phases of compiler and the design issues involved in compilation, code optimization techniques, machine code generation, and use of symbol table.
- To extend the knowledge of parser by parsing LL parser and LR parser. 4. To provide practical programming skills necessary for constructing a compiler.

Syllabus

Introduction to programming language translation. Lexical analysis: Specification and recognition of tokens.

Syntax analysis: Top-down parsing-Recursive descent and Predictive Parsers. Bottom-up ParsingLR (0), SLR, and LR (1) Parsers.

Semantic analysis: Type expression, type systems, symbol tables and type checking. Intermediate code generation: Intermediate languages. Intermediate representation-Three address code and quadruples. Syntax-directed translation of declarations, assignments statements, conditional constructs and looping constructs.

Runtime Environments: Storage organization, activation records. Introduction to machine code generation and code optimizations.

Lab Practice

Generation of lexical analyzer using tools such as LEX - Generation of parser using tools such as YACC - Creation of Abstract Syntax Tree-Creation of Symbol tables, Semantic Analysis - Generation of target code.

Text Books/References

1. Aho A.V., Lam M. S., Sethi R., and Ullman J. D., Compilers: Principles, Techniques and Tools, Pearson Education, 2007.
2. Appel A.W, and Palsberg J., Modern Compiler Implementation in Java, Cambridge University Press, 2002.
3. W. Appel, Modern Compiler Implementation in C, Cambridge University Press, 1998.
4. V. Aho, M. S. Lam, R. Sethi, J. D. Ullman, Compilers- Principles, Techniques & Tools, Second Edition, Pearson Education, 2007.

ICS 224 Computer Networks [3-0-3-4]

Course Objectives

- The students should understand the layers of networking devices.
- They should be familiar with a few networking protocols.
- They should study the different types of networks and topologies of networks.

Course Outcomes:

- To distinguish the importance of different networking components.
- To understand the functionalities of each networking layers and standards.
- To write simple networking-based programs at real and simulator level.

Syllabus

Evolution of computer networks: Network Architecture-OSI, TCP/IP models.

Physical and Data link layer: Encoding, Framing, Error detection, HDLC, PPP, sliding window protocols, medium access control, Token Ring, Wireless LAN, Packet Switching.

Network Layer: Internet addressing, IP, ARP, ICMP, CIDR, Routing algorithms (RIP, OSPF, BGP).

Transport Layer: UDP, TCP, flow control, congestion control Introduction to quality of service.

Application Layer: DNS, Web, HTTP, email, authentication, encryption.

Lab Practice

Unix network measurement and analysis tools, NS3 Socket interface and programming, RPC, RMI, Assignments using Network Simulators.

Texts Books /References

1. L. L. Peterson and B. S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Elsevier, 2011.
2. A. S.Tanenbaum and D.J. Wetherall, Computer Networks, Fifth Edition, Pearson, 2011.
3. W. R. Stevens, UNIX Network Programming, Volume 1: Networking APIs: Sockets and XTI, Second Edition, PrenticeHall,1998.
4. S. S. Panwar, S. Mao, J. Ryoo, and Y. Li, TCP/IP Essentials: A Lab-based Approach, Cambridge Press, 2004.
5. J. F. Kurose and K. W. Ross, Computer Networking: A Top Down Approach, Seventh Edition, Pearson India, 2017.
6. D. E. Comer, Internetworking with TCP/IP Vol. 1, Sixth Edition, Prentice Hall of India, 2006.
7. B. Forouzan, Data Communications and Networking, Fifth Edition, Tata Mcgraw Hill, 2012.
8. Introduction to Network Simulator NS2, Second Edition, 2011.

IMA221 Differential Equations and Transforms [3-1-0-4]

Course Objectives

- Find the Fourier series representation of a function of one variable
- Introduce the Fourier series and its application to the solution of partial differential equations
- Introduce the concepts of Laplace and Fourier transforms.
- Identify the type of a given differential equation and select and apply the appropriate analytical technique for finding the solution of first order and selected higher order ordinary differential equations.
- Introduce students to partial differential equations
- Introduce students to how to solve linear Partial Differential with different methods.

Course Outcomes

- Analyse and solve engineering problems using Fourier series.
- Find the Laplace and Fourier transforms of functions of one variable.
- Solve first order differential equations utilizing the standard techniques for separable, exact, linear, homogeneous, or Bernoulli cases. Find particular solutions

when given initial or boundary conditions.
- Will be able to find solution of higher-order linear differential equations
- Classify PDEs, apply analytical methods, and physically interpret the solutions

Syllabus

Fourier Series : Dirichlet's conditions – General Fourier series – Odd and even functions – Half range Sine and Cosine series – Complex form of Fourier series – Parseval's identity – Harmonic Analysis. Convergence of FS, differentiation and integration of Fourier series.

Fourier Transform Fourier Integral Theorem – Fourier transform pair - Sine and cosine transforms – Properties – Transform of elementary functions – Convolution theorem – Parseval's identity.

Ordinary Differential Equations: Method of variation of parameters – Method of undetermined coefficients – Homogenous equation of Euler's and Legendre's type – System of simultaneous linear differential equations with constant coefficients.

Partial Differential Equations Formation – Solutions of first order equations – Standard types and Equations reducible to standard types – Singular solutions – Lagrange's linear equation – Integral surface passing through a given curve – Classification of partial differential equations - Solution of linear equations of higher order with constant coefficients – Linear non-homogeneous

Fourier Series Solutions Of Partial Differential Equations: Method of separation of variables – Solutions of one dimensional wave equation and one dimensional heat equation – Steady state solution of two-dimensional heat equation – Fourier series solutions in Cartesian coordinates.

Text Books/References

1. C. Edwards and D. Penney, Elementary Differential Equations with Boundary Value Problems, 6th edition, Pearson, 2003
2. W.E. Boyce and R.C. DiPrima, Elementary Differential Equations, 7th Ed., John Wiely& Sons, 2002.
3. Erwin Kreyszig, Advanced Engineering Mathematics, 10th Edition, Wiley, 2015.
4. Tyn Myint-U, L.Debnath, Linear Partial Differential Equations for Scientists and Engineers, 4th Edition, Birkhauser, 2007.

IHS 221 Fundamentals of Economics [1-0-0-1]

Course Objectives

- To familiarize the participants concepts and techniques in Economics
- To make the participants appreciate the applications of core concepts in economics for managerial decision making
- To sensitize the participants how economic environment affects Organizations

Course Outcome

- It will help the students to analyse the demand and supply conditions and assess the positions of a company.
- It will help to design competition strategies, including costing, pricing, product differentiation and market environment according to the natures of products and structures of market

Syllabus

Introduction to Fundamentals of Economics

Micro & Macro Economics, Managerial Economics – Definition – Nature & Scope, Fundamental concepts in Managerial economics for decision making: Incremental Principle, Opportunity Cost, Discounting Principle, Time Concept, Equi-Marginal Principle – Illustrations, Decision Making – Process and Conditions – Difference between Risk & Uncertainty.

Demand Analysis and Forecasting

Meaning of Demand – Types of Demand – Law of Demand & its Exceptions, Elasticity of Demand – Price Elasticity, Income Elasticity, Cross Elasticity, Promotion Elasticity, Applications of the concepts of Elasticity, Demand Forecasting – Process – Statistical & Non-Statistical Techniques, Utility Analysis & Consumer Behaviour – Equilibrium of the consumer using Cardinal & Ordinal Utility (Indifference Curve) Theories.

Supply & Production

Theory of Production – Meaning of Production function, Production function with one variable input – Law of Variable Proportions – Returns to Scale, Production function with two variable inputs – Iso-quants – Producers' Equilibrium, Economies of Scale – Types – Economies of Scope, Theory of Costs – Classification of Costs

- Short Run & Long Run Cost Curves, Revenue Curves.

Market Structure

Market – Meaning & Elements, Classification of Markets – Markets based on Competition, Theory of Firm – Profit Maximization Rules, Price & Output Determination under Perfect Competition, Price & Output Determination under Monopoly – Monopoly Price Discrimination, Price & Output Determination under Monopolistic Competition, Price & Output Determination under Oligopoly – Kinked Demand curve model only.

Macro-Economic Concepts

National Income Concepts – Measurement of National Income, An overview of Financial System in India, An overview of Fiscal & Monetary Policies in India, Balance of Payments: Causes of Disequilibrium & Remedies, Inflation in India – Causes & Remedies. Free Market Economy & Need for Government Intervention – An appraisal of Economic Reforms in India

Text Books/ References

1. Dwivedi D.N, Managerial Economics, Vikas Publications (ISBN 8125910042)
2. P.L. Mehta, Managerial Economics Analysis, Problems and Cases – Sultan Chand & Sons (ISBN 81-7014-386-1)
3. K.K. Dewett, Modern Economic Theory: Micro & Macro Analysis – Orient Book Distributors, New Delhi.
4. V.L. Mote, Managerial Economics – Tata McGraw Hill, New Delhi
5. Gaurav Dutt & Aswani Mahajan, Dutt &Sundaram's Indian Economy – Sultan Chand & Sons

IHS 223 Risk Management [1-0-0-1]

Course Objectives

To explore financial and credit risk, decision making and corporate security and insurance.

Course Outcome

This course equips you with the skills to apply project risk management principles to a range of sectors.

Syllabus

Module 1 Sources and Types of business risk – Implications of business risk-risk perception of individuals and institutions-Alternatives for managing financial risk –diversification – reinsurance – contingency contracts Derivatives in the Indian Context – Trading infrastructure.

Module II Risk Management using derivatives-Forwards and Futures –Commodity Futures Financial Derivatives- Stock Futures and Index Futures – Interest Rate Futures – Currency Futures – Designing Futures Contracts – Hedging Positions in Futures.

Module III Stock options – Basic Properties of Options –Stock and Index Options Valuation– Sensitivity of Option Prices - Binomial Option Pricing – Black and Scholes Option Pricing using

Black and Scholes Formula-Trading strategies using options –Hedging Positions in Options - Synthetic options and portfolio insurance.

Module IV Interest rate swaps; forward rate agreements and interest rate futures.

Module V Accounting and Administration of Derivatives - Regulation of derivatives activity.

Textbooks/References

1. John C Hull "Fundamentals of Futures and Options Markets," Pearson, seventh edition.
2. Elton Edwin J and Gruber Martin J, Modern Portfolio Theory and Investment Analysis, John Wiley & Sons.
3. Russel Fuller, Modern Investments and Security Analysis, McGraw Hill.

ICS 225 Data Structure III [1-0-3-2]

Course Objectives

- Ensure that the student evolves into a competent programmer capable of designing and analyzing implementations of algorithms and data structures for different kinds of problems.
- Expose the student to the algorithm analysis techniques.

Course Outcomes

- Analyze the efficiency of programs based on Complexity.
- Understand the necessary mathematical abstraction to solve problems.

Syllabus

Algorithms on Graph connectivity but not limited to: Tarjan's and Kosaraju's strongly

connected components algorithms, Detect cycles in an undirected graph, Degree of vertices in a Graph, Path identification between vertices in Undirected graph.

Discussions on Randomized algorithms but not limited to: Reservoir Sampling, Birthday Paradox, Load Balancing problem, Karger's algorithm for Minimum Cut, Freivald's Algorithm to check the product of a matrix, Monte Carlo estimation.

Branch and Bound Algorithms: Knapsack problem, Travelling salesman problem.

Threaded Binary Tree, Splay trees, Foldable binary trees, Additional problems on BST, Binomial heap, Fibonacci heap, Topological sorting, self-organizing tree, segment tree, Binary indexed tree, suffix array and suffix tree, pattern searching , Tribonacci word.

Text Books/References:

1. Cormen, Thomas H., et al. Introduction to algorithms. MIT press, 2009.
2. Aho, Albred V., J. E. Hopcroft, and J. D. Ullman. "Data structures and algorithms (1983).
3. Drozdek, Adam. Data Structures and algorithms in C++. Cengage Learning, 2012.
4. Allen, Weiss Mark. Data structures and algorithm analysis in C++. Pearson Education India, 2007.
5. Kleinberg, Jon, and Eva Tardos. Algorithm design. Pearson Education India, 2006.
6. Skiena, Steven S. The algorithm design manual. Springer International Publishing, 2020.
7. Knuth, Donald Ervin. The art of computer programming. Vol. 3. Pearson Education, 1997.
8. Nomura, Seiichi. "C Programming and Numerical Analysis: An Introduction." Synthesis Lectures on Mechanical Engineering 2.2 (2018): 1-198.
9. Dasgupta, Sanjoy, C. H. Papadimitriou, and U. V. Vazirani. "Algorithms; 2006."
   Trefethen, Lloyd N., and David Bau III. Numerical linear algebra. Vol. 50. Siam, 1997.

SEMESTER V

CBS 311 Database Security [3-0-0-3]

Prerequisite for the Course
Student should have a passing grade in Database Management System (ICS 213) or the instructor's approval.

Course Objectives
- Introduce the database and its security issues.
- Compare in details the various state-of-art database security methods and techniques.
- Learn in detail the security features in databases.
- Understand the database monitoring tools.

Expected Outcome
Students who successfully complete this course will be able to:-
- Understand and characterize modern techniques of database information security threats and techniques for database security assessment.
- Analyze information in a database to identify information security incidents.
- Understand and use the main tools for database management systems monitoring.
- Apply build-in database functions to enable database integrity support.
- Create a plan for vulnerabilities detection and identification in databases.

Syllabus
Introduction-Database System Applications, Purpose of Database Systems, View of Data - Data Abstraction, Instances and Schemas, ER diagrams, Introduction to the Relational Model - Querying relational data, Form of Basic SQL Query - Examples of Basic SQL Queries.

Introduction to database security issues- The role of databases in information systems. Access control management features. Cryptographic data protection. SQL language features, Statistical databases.

Database security methods and techniques- Access control to database objects: tables, attributes, records. Triggers, views, data masking. Cryptographic methods of protection. Escaping queries to a database. Change Tracking. Data integrity in the databases. Database backups.

Security features in databases- SQL statements for access control. Integrity (domain, attributes, tables, referential). Database monitoring tools.

References

1. Basta A., Zgola M, "Database Security" 3nd Edition, Cengage Learning, US, 2011
2. Ron Ben Natan, "Implementing database security and auditing", Digital Press, 2005.
3. Bhavani Thuraisingham, Database and Applications Security, Auerbach Publications, 2005.
4. Rose Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.
5. Michael Gertz, Sushil Jajodia, Handbook of Database Security Applications and Trends, Springer, 2008.
6. Silvana Castano, Database Security, ACM Press.
7. Alfred Basta, Melissa Zgola, Database Security, Cengage Learning.

IEC 312 Distributed System Security [3-0-3-4]

Course Objectives
- To understand different levels of security threats in distributed systems
- To learn the security solutions for each layer security threads
- To design a secure distributed system

Expected Outcome

Students who successfully complete this course will be able to:-

- Understand the threats against distributed systems and how to protect against them
- Have a foundation for designing and developing secure distributed systems, and for evaluating the security of existing solutions
- Have knowledge of standards, security protocols, technologies, principles, methods and cryptographic mechanisms applicable for securing modern distributed systems
- Have knowledge of common mistakes leading to insecurities in distributed systems

Syllabus

Introduction- Background, Distributed Systems, Distributed Systems Security, Common Security Issues and Technologies

Host-Level Threats and Vulnerabilities- Background, Malware, Eavesdropping, Job Faults, Resource Starvation, Privilege Escalation, Injection Attacks.

Infrastructure-Level Threats and Vulnerabilities- Introduction, Network-Level Threats and Vulnerabilities, Grid Computing Threats and Vulnerabilities, Storage Threats and Vulnerabilities, Overview of Infrastructure Threats and Vulnerabilities.

Application-Level Threats and Vulnerabilities- Introduction, Application-Layer Vulnerabilities.

Service-Level Threats and Vulnerabilities- SOA and Role of Standards, Service-Level Security Requirements, Service-Level Threats and Vulnerabilities, Service-Level Attacks, Services Threat Profile.

Host-Level Solutions- Sandboxing, Virtualization, Resource Management, Proof-Carrying Code, Memory Firewall, Antimalware.

Infrastructure-Level Solutions- Network-Level Solutions, Grid-Level Solutions, Storage-Level Solutions.

Application-Level Solutions- Application-Level Security Solutions.

Service-Level Solutions- Services Security Policy, SOA Security Standards Stack, Deployment Architectures for SOA Security.

References

1. Belapurkar, A., Chakrabarti, A., Ponnapalli, H., Varadarajan, N., Padmanabhuni, S., & Sundarrajan, S. (2009). Distributed systems security: issues, processes and solutions. John Wiley & Sons.
2. Suri, N. (2019). DISTRIBUTED SYSTEMS SECURITY KNOWLEDGE AREA.
3. Firdhous, M. (2012). Implementation of security in distributed systems-a comparative study. arXiv preprint arXiv:1211.2032.
4. Burns, B. (2018). Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. " O'Reilly Media, Inc.".
5. Tanenbaum, A. S., & Van Steen, M. (2007). Distributed systems: principles and paradigms. Prentice-hall.

CBS 312 Network Security, IoT and Wireless Security [3-0-3-4]

Prerequisite for the Course

Student should have a passing grade in, Computer Networks (ICS 224) Digital Design and Electric Circuits (IEC 121) Computer Programming (ICS 112) or the instructor's approval.

Course Objectives

- Introduce the concept and the basics of Wireless, IoT and Cloud technologies.
- Analyze various secured Wireless Communication Protocols for IoT Infrastructure.
- Provide knowledge on various applications of IoT based technologies and their associated circuits.
- Enable awareness on the different IoT Vulnerabilities, Attacks, and security methods.

Expected Outcome

Students who successfully complete this course will be able to:-

- Learn the basics of communication in wireless sensor network, Cloud Computing.
- Compare various secured Wireless Communication Protocols for IoT Infrastructure.
- Understand the various applications of IoT,
- Design IoT based applications using Arduino or Raspberry PI boards.
- Understand the various attacks and different security measures in IoT infrastructure.

Syllabus

Introduction - Basics of networking - wired, wireless, MANET, PAN, Wireless Sensor Networks, M2M Communication.

Secured Wireless Communication Protocols for IoT Infrastructure- IPv6 - LowPAN, LoRa, Transport-Bluetooth-LPWAN, Data -MQTT –CoAP.

IoT architectures and programming - basic architectures, Sensor basics, sensing and actuation, sensor communications, connectivity challenges Data processing mechanisms, scalability issues, visualization issues, analytics basics, utility of cloud computing, fog computing, and edge computing, advanced IoT architectures Raspberry Pi and Arduino programming.

Applications - IoT for industrial automation (Industry 4.0), smart city, smart home, smart transportation, smart healthcare, smart agricultures, golang based implementation.

IoT security: Vulnerabilities, Attacks, and countermeasures, security engineering for IoT development, IoT security lifecycle.

References

1. Pethuru Raj and Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press, First edition, 2017.
2. B. Rusell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.
3. Fei HU, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, andImplementations”, CRC Press,2016
4. Honbu Zhou, The Internet of Things in the Cloud: A Middleware Perspective, CRC press, First edition, 2012.
5. Arshdeep Bahga and Vijay Madisetti, Internet of Things: A Hands-on Approach, Universities Press, First edition, 2014.
6. Mung Chiang, Bharath Balasubramanian, Flavio Bonomi, Fog for 5G and IoT (Information and Communication Technology Series, Wiley series, First edition, 2017.
7. Alan A. A. Donovan, Brian W. Kernighan, The Go Programming Language, AddisonWesley Professional Computing Series, First edition, 2015.

CBE 3311 Fundamentals of Data Science [3-0-3-4]

Prerequisite for the Course

Student should have a passing Grade in Calculus and Linear Algebra (IMA 121), Probability, Statistics and Random Processes (IMA 211) and Data Structures I (ICS 121) or the instructor’s approval.

Course Objectives

- To introduce the concepts, techniques and methodologies in data science.
- To provide skills required to uncover patterns and underlying relationships in small data.
- To introduce classical data mining techniques and related tools.
- To impart basic concepts of recommender systems.

Expected Outcome

- Comprehend the various phases involved in the data science process.
- Apprehend the differences between related tasks in data science.
- Ability to perform data pre-processing and data visualization.

- Ability to design and develop classification systems for real-world problems.
- Ability to perform clustering analysis.
- Ability to design and implement recommender systems.

Syllabus

Review: Concepts of linear algebra, Matrix factorization, Statistics: Random variables, Distributions and limit theorems, Stochastic processes, Hypothesis testing.

Introduction: Overview of Data Science: Knowledge Discovery and machine learning vs data mining, Data Science process, Data pre-processing and cleaning: Data integration and transformation, Feature engineering and extraction, Data sampling, Data reduction, Data discretization, Outlier detection, Knowledge mining from databases, Similarity measures.

Data mining algorithms and techniques: Overview of data mining process, Data mining strategies: Classification and prediction: Classification using Decision Trees – Ensemble Data Mining, Anomaly Detection, Mining association rules and frequent patterns: concepts and methods, Cluster analysis, Mining unstructured and semi-structured data.

Data Analytics and visualization: Data summarization, Exploratory data Analysis (EDA): tools and techniques, application of transforms for data analysis.

Recommender Systems and Collaborative Filtering: Taxonomy of recommender systems, Content-based Recommendation, Neighborhood-based recommendation, Memory-based Collaborative Filtering, Model-based Collaborative Filtering.

Programming labs:

Manipulating and visualizing data with R, Outlier detection, Statistical analysis on data, Data wrangling and cleaning, Probability Distributions, Analysis of variance, Feature engineering and extraction, Data mining algorithms: Classification, Clustering, Frequent pattern and association rule mining, Recommender systems.

References

1. Jiawei Han. “Data Mining: Concepts and Techniques”. Morgan Kaufmann Publishers.
2. Tan, Pang-Ning, Michael Steinbach, and Vipin Kumar. “Introduction to data mining”. Pearson Education India, 2016.
3. Ricci, Francesco, Lior Rokach, and Bracha Shapira. "Introduction to recommender systems handbook." Recommender systems handbook. Springer, Boston, MA, 2011.
4. Witten, E. Frank, M. Hall. “Data Mining: Practical Machine Learning Tools and Techniques”, Morgan Kaufmann Publishers, 2011.
5. Garett Grolemund, Hadley Wickham. “R for Data Science”. O’Reilly Media Inc. 2016.
6. Cichosz, Pawel. Data mining algorithms: explained using R. John Wiley & Sons, 2014.

IMA 312 Number Theory and Mathematical Theory of Coding [3-0-0-3]

Course Objectives

- To understand the basics of number theory, theory of congruences and modular arithmetic and to apply the same in data security.
- To analyse various error correction codes.

Expected Outcome

Students who successfully complete this course will be able to:-

- Apply the basics of number theory in different scenario.
- Learn different error correcting codes.

Syllabus

Introduction to number theory: Theory of congruences and applications Divisibility theory - division algorithm, the greatest common divisor, the Euclidean algorithm, the Diophantine equation- Primes and their distribution – the fundamental theorem of arithmetic (no proof) and applications: The theory of congruences – binary and decimal representation of integers, congruences in one unknown, Chinese remainder theorem, Fermat’s theorem, pseudo primes, Fermat factorization.

Number theoretic functions: Numbers of special form Number theoretic functions - the sum and number of divisors, the greatest integer function, an application to the calendar, Euler’s phi function, Euler’s theorem: Numbers of special form – perfect numbers, Fermat numbers, Legendre symbol, Jacobi symbol.

Algebraic structures: Finite fields The order of integer modulo, Primitive roots, discrete logarithms, quadratic residue, quadratic reciprocity law, primality testing: Introduction to groups, rings and fields: Polynomial arithmetic, finite fields.

Introduction to coding theory: Error correcting codes Basic concepts and definitions, encoding and decoding, bounds on general codes, linear codes, syndrome decoding, the dual code, Hamming codes, cyclic codes, Reed-Solomon codes.

References

1. D. A. Burton, Elementary Number Theory, 6/e, Tata McGraw Hill, 2007.
2. Stallings W., Cryptography and Network security: Principles and Practice, 4/e, Pearson Education Asia, 2006.
3. Wade Trappe, Lawrence C. Washington, Introduction to Cryptography with Coding Theory, Second Edition.
4. Niven I., Zuckerman H. S. and Montgomery H. L., An Introduction to Theory of Numbers, 5/e, John Wiley and sons, 2004.
5. Joseph A. Gallian, Contemporary Abstract Algebra, Narosa, 1998.

IHS 314 Financial crime, Motivations and Typologies [3-0-0-3]

Course Objectives

- To understand the tracing illicit financial Transactions and various anti-money laundering laws.
- To analyse various schemes of Insurance fraud.
- To understand Bankruptcy schemes, methods of proving corrupt payments and bribery.

Expected Outcome

At the end of course candidates should be able to:

- Understand Tracing Illicit financial Transactions.
- Understand the various anti-money laundering laws.
- Explain the various schemes of insurance fraud.
- State and explain Bankruptcy schemes.
- Explain the methods of proving corrupt payments and bribery.

Syllabus

Tracing Illicit Transactions:

Identify the common areas of interview questions in tracing financial crime evidence- State and explain the main sources income and expenditure of illicit financial crime- Distinguish between the direct and indirect methods of tracing illicit financial transactions- Describe the investigation procedures for tax fraud - Describe the indirect method of tracing financial crime- Describe the Net worth Method of investigating financial crime- Prepare a profile of a financial fraudster-Determine the net worth of a financial crime suspect.

Anti-Money Laundering Laws

Define Money Laundering and Identify the process of money laundering - Identify the Major Money Laundering Countries in the World- Explain Money Laundering and describe the penalty for Money Laundering under the Money Laundering Act- Describe the Composition of the Financial Intelligence Centre- Define Accountable Institutions - State and explain the composition of accountable institutions- Identify the various International bodies that imposes Money Laundering Sanctions- State and Explain the various of types of Money Laundering Sanctions.

Law Enforcement and Financial Crime-Identify when law enforcement agencies generally are called in to assist with a financial crime investigation.

Insurance and Medical Fraud

Define insurance fraud- State and explain the types of insurance policies-State and explain the various schemes of insurance fraud- Identify the red flags associated with insurance fraud- State and explain the types of insurance fraud investigation tips- Define medical fraud- State and explain the types of medical fraud schemes.

Bankruptcy

Define Bankruptcy- Identify the red flags associated with bankruptcy-State and explain Bankruptcy schemes- Define Planned Bustout and state its characteristics- State and Explain the objectives of the world bank principles on effective insolvency- State and Explain the legal framework for creditor rights and Insolvency.

Bribery and Corruption

Define bribery and corruption-State and explain kickback schemes-State and explain the methods of making illegal payments- State and explain the types of procurement fraud schemes- Identify the red flags associated with bribery and

corruption- State and explain the methods of proving corrupt payments- Prove Ghost employee schemes in a given scenario.

References

1. Expert Fraud Investigation; a step-by-step guide by Tracy L. Coenen
2. ACFE Fraud Examiners Manual
3. IICFA Study Manual
4. A Practitioner's Guide to the Law and Regulation of Financial Crime by Arun Srivastava and Andrew Keltie, 2010
5. Anti-Money Laundering Act
6. Forensic Criminology by Wayne A. Petherick, Brent E. Turvey, Claire E. Ferguson, 2009
7. Insurance Fraud Casebook, Paying a premium for crime by Joseph T. Wells and Laura Hymes

CBE 3312 Introduction to Artificial Intelligence [1-0-0-1]

Prerequisite for the Course

Student should have a passing Grade in Data Structures I (ICS 121), Design and Analysis of Algorithms (ICS 211) or the instructor's approval.

Course Objectives

- To provide a historical perspective and broad introduction to Artificial Intelligence (AI)
- To introduce the fundamental concepts and principles of AI for problem solving, knowledge representation and learning, and inference
- To provide a solid grounding of fuzzy logic and related concepts
- To impart knowledge on Expert systems tools and applications

Expected Outcome

- Demonstrate in-depth understanding of the fundamentals of AI
- Ability to solve basic problems by applying concepts of problem solving, knowledge representation and learning, and inference
- To design solutions for optimization problems using fuzzy logic or genetic algorithms
- Apply AI techniques to develop expert systems

Syllabus

Evolution and Fundamentals of AI: History of Artificial Intelligence (AI) and its applications, Agents, Problem Spaces and Search - Uniformed and informed search, Problem solving- Adversarial search and games, Search spaces - Weak methods, game trees

Knowledge Representation and Learning: Propositional logic, Predicate logic, Constraint-satisfaction problems

Uncertainty Reasoning: Bayesian Networks, Fuzzy logic-Membership functions, Fuzzy inference systems, Fuzzy knowledge and rule-based system

Expert Systems: Overview of expert systems, Inference, Forward chaining and backward chaining.

References

1. Stuart Russell, Peter Norvig, "Artificial intelligence: A Modern Approach", Prentice Hall, Fourth edition, 2020.
2. Luger, George F. Artificial intelligence: structures and strategies for complex problem solving. Pearson education, 2005.
3. Nils J. Nilsson, "Artificial Intelligence: A New Synthesis", Morgan-Kaufmann, 1998.
4. Elaine Rich, Kevin Knight: "Artificial intelligence". McGraw-Hill, Second edition, 1991
5. Timothy J. Ross, "Fuzzy Logic with Engineering Applications", John Wiley and Sons, Third edition, 2011.

SEMESTER VI

CBS 321 Machine Learning and Cyber Security [3-0-0-3]

Course Objectives

- To provide basic understandings on core concept of machine learning and its process.
- To provide an in-depth introduction to supervised, unsupervised and its application to specific security problems.
- To design and implement machine learning solutions to various security applications.

Expected Outcome

- Understand machine learning and its benefits in specific security problems.
- Learn the machine learning techniques such as supervised and unsupervised algorithms.
- Learn the use of machine learning for detecting and mitigating cyber threats in various applications.
- Develop an ability to select the appropriate machine learning algorithms to be used for specific security applications to tackle the security problem efficiently.

Syllabus

Machine Learning Overview: Introduction, Linear Regression, MLE, bias/variance trade-offs, technical requirements (Data pre-processing, standardization, dimension reduction, feature selection, Train-Test splitting, loss function, optimization, model selection, cross validation)

Supervised Learning: Naive Bayes classifier, support vector machine, Regularization, Classification errors, Decision Tree, K-nearest neighbours, Artificial Neural Network (ANN)

Unsupervised learning: Clustering (K-means, K-medoids, hierarchical clustering algorithms, BDSCAN)

Machine Learning for Malware detection, Supervised Learning for Misuse/Signature Detection, Anomaly Detection using ML, Spam detection based on Machine Learning approach, Adversarial Machine Learning

References

1. Mitchell, Tom. Machine Learning. NewYork, NY: McGraw-Hill, 1997.
2. Bishop, C. ,M., Pattern Recognition and Machine Learning, Springer, 2006
3. P. Langley, Elements of Machine Learning, Morgan Kaufmann, 1995.
4. Hastie, T., R. Tibshirani, and J. H. Friedman. The Elements of Statistical Learning:
5. Data Mining, Inference and Prediction, Second Edition, Springer, 2009
6. Dua, Sumeet, and Xian Du. Data mining and machine learning in cybersecurity. CRC press, 2016.
7. Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. “O’Reilly Media, Inc.", 2018.

CBS 322 Digital Forensics [3-0-3-4]

Prerequisite for the Course

Student should have a passing Grade in IT Workshop I (ICS111) and Operating Systems (ICS 212) or the instructor’s approval.

Course Objectives

- Summarize the basic principles of computer forensics.
- Understand various stages of digital forensics investigation.
- Summarize important laws relevant to digital forensics investigation.
- Describe the digital forensic lab and tools.
- Understand storage management and its importance in forensics
- Understand the file system fundamentals and the internals of Windows and Linux file systems.

Expected Outcome

Students who successfully complete this course will be able to:-

- Understand the principles and stages of computer forensics.
- Comprehend various legal aspect pertaining to digital forensic investigation.
- Understand various Windows and Linux Files systems and its operations.
- Grasp digital forensic tools and the setup of a digital forensic lab.

Syllabus

Introduction to Computer Forensics, Foundations of Digital Forensics, Need for Digital Forensics, Forensic Investigation Model.

Overview of computer hardware and operating systems, Storage media/devices and their working, Windows and Linux File Systems.

First Responder, Forensic data acquisition, Forensic data validation, Evidence Collection and Analysis Techniques, Disk Wiping.

Computer crimes and Legal issues.

References

1. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, 6th Edition, Publisher: Cengage Learning.
2. Chuck Easttom, System Forensics Investigation and Response, 3rd Edition, Publisher: Jones & Bartlett Learning.
3. Cory Altheide, Bruce Nikkel, Harlan Carvey, Digital Forensics with Open Source Tools, Publisher: Elsevier publication.
4. Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, Publisher: Pearson.
5. Cory Altheide, Bruce Nikkel, Harlan Carvey, Digital Forensics with Open Source Tools, Publisher: Elsevier Science & Technology.

CBE 3321 Cloud Computing and Security [3-0-3-4]

Course Objectives

- Understand core cloud computing concepts and fundamental principles, including standard delivery models and service designs.
- Understand the foundational security practices that are required to secure modern cloud computing infrastructures.
- Understand the differences between traditional data security practices and cloud-based data security methodologies.
- Understand the identity and access management practices of both cloud providers and consumers.
- Understand how to protect data-at-rest, data-in-transit, and data-in-use within a cloud environment.
- Understand the complexity of cloud threat actors and techniques used to attack a cloud computing infrastructure.

Expected Outcome

Students who successfully complete this course will be able to:-

- Comprehend the fundamentals of cloud computing architectures
- Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud
- Design approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on-demand computing, shared resources, elasticity and measuring usage.
- Apply security architectures that assure secure isolation of physical and logical infrastructures.

Syllabus

Fundamentals of Cloud Computing and Architectural Characteristics- Cloud computing Architectural- Cloud deployment models Public, Private, Community and Hybrid models Scope of Control Software as a Service (SaaS) Platform as a Service (PaaS) Infrastructure as a Service (IaaS)- Cloud Computing Roles Risks.

Security Concepts, Defence in depth, Importance in PaaS, IaaS and SaaS- User authentication in the cloud- Cryptographic Systems- Key management, X.509 certificates, OpenSSL.

Multi-Tenancy Issues: Isolation of users/VMs, Virtualization System Security Issues- ESX and ESXi Security, ESX file system security, storage considerations, backup and recovery.

Virtualization System Vulnerabilities, Virtualization System-Specific Attacks, Virtualization-Based Security Enhancement: virtual server protection, virtualization-based sandboxing; Storage Security- HIDPS, log management, Data Loss Prevention. Location of the Perimeter.

References

1. Cloud computing a practical approach - Anthony T.Velte , Toby J. Velte Robert Elsenpeter, TATA McGraw- Hill , New Delhi – 2010
2. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online - Michael Miller - Que 2008
3. Tim Mather, Subra Kumaraswamy, ShahedLatif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance” O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.
4. Ronald L. Krutz, Russell Dean Vines, “Cloud Security” [ISBN: 0470589876], 2010.
5. John Rittinghouse, James Ransome, “Cloud Computing” CRC Press; 1 edition [ISBN: 1439806802], 2009.

6. J.R. ("Vic") Winkler, “Securing the Cloud” Syngress [ISBN: 1597495921] 2011.
7. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing” 2009.
8. Vmware “VMware Security Hardening Guide” White Paper, June 2011 .
9. Cloud Security Alliance 2010, “Top Threats to Cloud Computing” Microsoft 2013. 8. Timothy Grance; Wayne Jansen;NIST “Guidelines on Security and Privacy in Public Cloud Computing”, 2011.

CBS 323 Cryptography [3-0-3-4]

Prerequisite for the Course
Student should have a passing Grade in Number Theory and Mathematical Theory of Coding (IMA 312), Discrete Mathematics (IMA 111).

Course Objectives
- To lay a foundation on Security in Networks, Classical Cryptosystem and Block Cipher Modes of Operation.
- To analyse various Private and Public key Cryptosystem for encryption, key exchange and hashing, Authentication Protocols.
- To acquire the fundamental knowledge on applications of cryptography.

Expected Outcome
Students who successfully complete this course will be able to:-
- Understand the fundamental concepts of Classical and modern Cryptosystem.
- Compare various private and public key Cryptosystem for encryption, key exchange and authentication algorithms.
- Understand the different applications of cryptography.

Syllabus
INTRODUCTION – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, Vignere cipher, substitution, transposition techniques,

BLOCK CIPHERS AND MODES OF OPERATIONS- DES - Data Encryption Standard-Block cipher principles-block cipher modes of operationAES-TripleDES-Blowfish-RC5

PUBLIC KEY CRYPTOGRAPHY- Public Key Cryptosystem, Key distribution, Diffie Hellman Key Exchange-MITM Attack - RSA, Random Number Generation-ECC-Key Management

HASH FUNCTIONS AND DIGITAL SIGNATURES- Authentication requirement– Authentication function – MAC – Hash function – SHA - HMAC - Digital signature and authentication protocols.

APPLICATIONS- Authentication – Kerberos, IP Security – IPSec, Web Security - SSL, TLS, Blockchain, IoT Security.

References
1. William Stallings, Cryptography and Network Security –6th Edition, Pearson Education.
2. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 5nd Edition, Mc Graw Hill Education.
3. Rich Helton, Johennie Helton, Mastering Java Security: Cryptography Algorithms and Practices, John Wiley Publishers.
4. Charles P. Pleeger, “Security in Computing”, Pearson Education Asia, 5th Edition.
5. William Stallings, “Network Security Essentials: Applications and standards”, Person Education Asia.
6. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security: Private Communication in a public world”, Prentice Hall India, 6nd Edition.

ISC 322 Criminal Psychology and Behavior Intelligence [3-0-0-3]

Course Objectives
To makes the students familiar with the field of Criminal Psychology.

To make the students understand the origins of Criminal Behaviour.

Expected Outcome
Students who successfully complete this course should have a comprehensive understanding of Criminal Behaviour and Psychology.

Syllabus
Nature and History of Criminal and Forensic Psychology, Social context of Crime: Extent of Criminality, Changing nature of Crime: Conservative and Radical interpretations in complexity of victimization.

Types of Offenders, Violent Offenders: Media influences and Research Statistics, Theories of

Homicide: Psychological disposition, Socio-Biological theory and Multi-Factorial Approach.

Mental Illness and Crime: Problem of evidence; Mental illness and Crime in general.

Eyewitness Testimony: Accuracy of witness evidence in Court, Witness confidence and improving the validity of line-up, Clinical approaches in Risk and danger assessment.

References

1. Dennis Howitt, Introduction to Forensic and Criminal Psychology, 6th Edition, Publisher: Pearson, 2018
2. Wayne Petherick Brent Turvey Claire Ferguson, Forensic Criminology, 1st Edition, Publisher: Elseiver, ISBN: 9780123750716
3. Bruce Arrigo Stacey Shipley, Introduction to Forensic Psychology, 2nd Edition, Publisher: Academic press, ISBN: 9780080468532

IOE 3321 Information Security Standards, Policies, Strategies & Audits [3-0-0-3]

Course Objectives

- Enable a clear understanding and knowledge of Security Analyst foundations.
- Expose students to various IT auditing techniques.
- Understand the significance of Risk Management.

Expected Outcome

Students who successfully complete this course should have a comprehensive understanding of Information Security Standards, auditing process and Risk Management.

Syllabus

Introduction and IT Audit, IT Environment, Methods for Business Advisory Audits, Role of the IT Audit Team, IT Audit Process, Identifying what to Audit, Stages of Auditing.

Auditing Techniques, Auditing Entity-Level Controls, Auditing Cybersecurity Programs, Auditing Data Centers and Disaster Recovery, Auditing Networking Devices, Auditing Windows and Linux Operating Systems, Auditing Web Servers and Web Applications, Auditing Databases, Auditing Storage, Auditing Virtualized Environments, Auditing End-User Computing Devices, Auditing Applications, Auditing Company Projects.

Frameworks, Standards, Regulations, and Risk Management, Internal IT controls, Benefits of Risk Management, Quantitative Risk Analysis, Qualitative Risk Analysis.

References

1. Mike Kegerreis, Mike Schiller, Chris Davis, IT Auditing Using Controls to Protect Information Assets, 3rd Edition, Publisher: McGraw-Hill Education, 2019, ISBN-10: 1260453227.
2. Angel R. Otero, Information Technology Control and Audit, 5th Edition, Publisher: Auerbach Publications, 2020, ISBN-10: 1498752284.
3. Martin Weiss, Michael G. Solomon, Auditing IT Infrastructures for Compliance, 2nd Edition, Publisher: Jones & Bartlett Learning, 2015, ISBN-10: 1284090701.
4. Stephen D. Gantz, The Basics of IT Audit: Purposes, Processes, and Practical Information, Publisher: Syngress, 2013, ISBN-10: 0124171591.

SEMESTER VII

CBE 4411 Mobile Forensics and Security [3-0-3-4]

Course Objectives

- To gain knowledge on mobile phone evidence extraction process
- To understand the practical mobile forensic approaches
- To engage students in forensic acquisition and analysis of mobile computing devices, specifically Android device
- To gain an understanding of mobile device identification

Expected Outcome

Students who successfully complete this course will be able to:-

- Understand what data is able to be acquire from mobile devices and be able to acquire and investigate data from mobile devices using forensically sound and industry standard tools.
- Comprehend the relationship between mobile and desktop devices in relationship to a criminal and corporate investigations.
- Analyse mobile devices, their backup files, and artifacts for forensic evidence.

Syllabus

Introduction to Mobile Forensics: Why do we need mobile forensics? Mobile forensics, Challenges in mobile forensics

The mobile phone evidence extraction, Documenting and reporting phase, Presentation phase, Archiving phase, Practical mobile forensic approaches: Overview of mobile operating systems, Data acquisition methods, Examination and analysis of evidence stored on mobile phones.

Understanding Android, Android model, Android security- Secure kernel, Security-Enhanced Linux, Full Disk Encryption, Trusted Execution Environment, Android file system.

Android Forensic Setup and Pre-Data Extraction Techniques, Android Data Extraction Techniques, Android Data Analysis and Recovery, Android data recovery, Android App Analysis, Malware, and Reverse Engineering: Analyzing Android apps; Reverse engineering Android apps; Extracting an APK file from an Android device; Android malware.

References

1. Bommisetty, Satish, Rohit Tamma, and Heather Mahalik. Practical mobile forensics. Packt Publishing Ltd, 2014.
2. Tamma, Rohit, and Donnie Tindall. Learning android forensics. Packt Publishing Ltd, 2015.
3. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.
4. Mikhaylov, Igor. Mobile Forensics Cookbook: Data acquisition, extraction, recovery techniques, and investigations using modern forensic tools. Packt Publishing Ltd, 2017.
5. Joakim, K. "Fundamentals of Digital Forensics. Theory, Methods, and Real-Life Applications, Springer International Publishing, Berlin, Heidelberg." (2018).

CBS 411 Penetration Testing, Vulnerability Analysis, IDS and Malware Analysis [3-0-3-4]

Prerequisite for the Course

Student should have a passing Grade in Computer Networks (ICS 224), Database Security (CBS 311) and Network Security, IoT and Wireless Security (CBS 312), or the instructor's approval.

Course Objectives

- Introduces the concepts of Penetration testing.
- Gives the students the opportunity to learn about different tools and techniques for penetration testing and security.
- Practically apply penetration testing tools to perform various activities.

Expected Outcome

Students who successfully complete this course will be able to:-

- Understand the core concepts related to vulnerabilities and their causes.
- Understand ethics behind hacking and vulnerability disclosure.
- Comprehend the impact of Hacking.
- Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies.

Syllabus

Introduction and Information Security Overview, Hacking and Ethical hacking concepts, Hacker behaviour & mindset, Hacking Methodology.

Footprinting Concepts and Methodology, Footprinting Tools and Countermeasures, Active and Passive Sniffing, Network Scanning Concepts and Tools, Preparation of Ethical Hacking and Penetration Test Reports and Documents.

Social Engineering attacks and countermeasures, Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing.

Metasploit framework, Penetration testing tools in Kali Linux.

References

1. Baloch, R., *Ethical Hacking and Penetration Testing Guide*, Auerbach Publications, CRC Press, 2015.
2. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, *Metasploit: The Penetration Tester's Guide*, No Starch Press, 2011, ISBN: 159327288X,9781593272883.
3. Sagar Rahalkar, *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*, 1st Edition, Apress publications, 2019, Softcover ISBN: 978-1-4842-4269-8.
4. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd Edition, Wiley Publisher, 2018, ISBN-13: 978-1119433385.
5. Glen D. Singh, *Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, And Wireshark*, Packt Publishing, 2019, ISBN: 1789611806.
6. Michael Hixon, Justin Hutchens, Kali Linux. Network Scanning Cookbook, Packt Publishing, 2017, ISBN: 139781787287907

CBS 412 Multimedia Security & Forensics [3-0-3-4]

Course Objective

- Introduce multimedia, its application areas, data encoding and compression techniques.
- Develop understanding of Quality of Service and its constraints.
- Understand synchronization concepts.
- Discuss multimedia security attacks and defense techniques.
- To introduce multimedia forensic concepts

Expected Outcome

Students who successfully complete this course will be able to:-

- Demonstrate how quality of service can be ensured in multimedia applications.
- Apply different synchronization techniques on multimedia.
- Ensure security of multimedia applications.
- Perform forensic on multimedia data

Syllabus

Introduction: Multimedia Application Areas, Interdisciplinary Aspects of Multimedia, Multimedia Data Encoding, Concept of data compression in multimedia field.

Quality of Service & Operating System: Requirements and Constraints, Quality of Services Concept, Resource Management, Media Server Architecture, Storage Management, Services, Protocols, Layers.

Security in Multimedia Applications: Security attacks, Multimedia Encryption, Steganography, Digital image watermarking, Multimedia Authentications.

Multimedia Evidence Handling: Digital Forensics Laboratories in Operation, Standards and Best Practices in Digital and Multimedia Forensics, Digital Evidence Extraction, Multimedia File Carving, Multimedia Device and Source Forensics: Forensic Camera Model Identification, Printer and Scanner Forensics, Microphone Forensics, Multimedia Content Forensics.

References

1. Ralf Steinmetz, Klara Nahrstedt. Multimedia Systems, Springer International Edition
2. Ho, Anthony TS, and Shujun Li, eds. Handbook of digital forensics of multimedia data and devices. John Wiley & Sons, 2015.
3. John. F. Koegel Buford. Multimedia Systems. Pearson Education.
4. Digital Watermarking and Steganography By Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica

5. Steinmetz, Ralf, Jana Dittmann, and Martin Steinebach, eds. Communications and Multimedia Security Issues of the New Century: IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01) May 21–22, 2001, Darmstadt, Germany. Vol. 64. Springer, 2013.

IOE 4411 Block Chain & Crypto-Currencies [3-0-0-3]

Prerequisite for the Course

Student should have a passing Grade in Computer Networks (ICS 224) or the instructor's approval.

Course Objectives

- Introduce the concept and the basics of blockchain technologies.
- Enable awareness on the different generations of blockchains.
- Provide knowledge on various applications of blockchain technologies.

Expected Outcome

Students who successfully complete this course will be able to:-

- Understand the basics of blockchain Technologies and its various applications.
- Implement blockchain ledgers.
- Capable to identifying problems on which blockchains could be applied.

Syllabus

Introduction – Blockchain history, basics, architectures, Types of blockchain, Base technologies – Dockers, Hash function, Digital Signature - ECDSA, Zero Knowledge Proof.

Bitcoins – Fundamentals, aspects of bitcoins, properties of bitcoins, bitcoin transactions, bitcoin P2P networks, block generation at bitcoins, consensus algorithms- Proof of Work, Proof of Stake, Proof of Burn.

Blockchain hyperledger – Fabric architecture, implementation, networking, fabric transactions, demonstration, smart contracts.

Applications – Blockchain applications, e-governance, smart cities, smart industries, anomaly detections, use cases, trends on Blockchains, serverless blocks, scalability issues, blockchain on clouds.

References

1. Baxv Kevin Werbach, The Blockchain and the new architecture of Trust, MIT Press, 2018.
2. Joseph J. Bambara and Paul R. Allen, Blockchain – A practical guide to developing business, law, and technology solutions, McGraw Hill, 2018.
3. Joseph J. Bambara and Paul R. Allen, Blockchain, IoT, and AI: Using the power of three to develop business, technical, and legal solutions, Barnes & Noble publishers, 2018.
4. Melanie Swan, Blockchain – Blueprint for a new economy, OReilly publishers, 2018.
5. Jai Singh Arun, Jerry Cuomo, Nitin Gaur, Blockchain for Business, Pearson publishers, 2019.
6. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

SEMESTER VIII

CBE 4421 Cyber Ethics, Privacy and Legal Issues [3-0-0-3]

Course Objectives

The course deals with all the aspects of Cyber law as per Indian/IT act. It also covers overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.

Expected Outcome

Students who successfully complete this course will be able to demonstrate a critical understanding of the Cyber law with respect to Indian IT/Act, Cyber Ethics and Intellectual Property Rights.

Syllabus

Cyber Crimes Categories and kinds, Evolution of the IT Act, IT Act, 2000, various authorities under IT Act and their powers. Penalties & Offences, amendments.

Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E –commerce and Laws in India, Digital / Electronic Signature in Indian Laws.

Intellectual Property Rights, Domain Names and Trademark Disputes, Copyright in Computer Programmes, Concept of Patent Right, Sensitive Personal Data or Information in Cyber Law, Cyber Law an International Perspective.

Cyber Ethics and Code, Net Neutrality, Free speech and Censorship in Cyberspace, Intellectual Property in Cyberspace, Privacy Rights and Surveillance.

References

1. Sushma Arora, Raman Arora, Cyber Crimes & Laws, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, Technology Laws Decoded, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723
3. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House New Delhi
4. P.M. Bukshi and R.K. Suri, Guide to Cyber and E –Commerce Laws, Bharat Law House, New Delhi
5. Rodney D. Ryder, Guide to Cyber Laws; Wadhwa and Company, Nagpur
6. The Information Technology Act, 2000; Bare Act –Professional Book Publishers, New Delhi
7. Richard A.Spinello, Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace, 7th Edition, Publisher: Jones & Bartlett Learning, 2020, ISBN-10: 1284184064

CBE 4422 Biometric Security [3-0-3-4]

Course Objective

- To understand the technologies of fingerprint, iris, face and speech recognition
- To understand the general principles of design of biometric systems and the underlying trade-offs.
- To recognize personal privacy and security implications of biometrics based identification technology.
- To identify issues in the realistic evaluation of biometrics based systems.

Expected Outcome

Students who successfully complete this course will be able to:-

- Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
- Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.
- Demonstrate knowledge engineering principles underlying biometric systems.
- Analyze design basic biometric system applications.
- Understand various Biometric security issues.

Syllabus

Biometrics: Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

Fingerprint Identification Technology: Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing – Minutiae Determination – Fingerprint Matching: Fingerprint Classification, Matching policies.

Face Recognition: Introduction, components, Facial Scan Technologies, Face Detection, Face Recognition, Representation and Classification, Kernel- based Methods and 3D Models, Learning the Face Spare, Facial Scan Strengths and Weaknesses, Methods for assessing progress in Face Recognition.

Fusion in Biometrics: Introduction to Multibiometric – Information Fusion in Biometrics – Issues in Designing a Multibiometric System – Sources of Multiple Evidence – Levels of Fusion in Biometrics – Sensor level, Feature level, Rank level, Decision level fusion – Score level Fusion.

Examples – Biopotential and gait based biometric systems.

Case Study Presentations: Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim, Identification Forensic Odontology.

References

1. James Wayman, Anil Jain, Davide Maltoni, Dario Maio, Biometric Systems, Technology Design and Performance Evaluation, Springer, 2005.
2. David D. Zhang, Automated Biometrics: Technologies and Systems, Kluwer Academic Publishers, New Delhi, 2000.
3. Arun A. Ross, Karthik Nandakumar, A.K.Jain, Handbook of Multibiometrics, Springer, New Delhi, 2006.
4. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : "Biometrics -Identity verification in a network", 1st Edition, Wiley Eastern, 2002.
5. John Chirillo and Scott Blaul : "Implementing Biometric Security", 1st Edition, Wiley Eastern Publication, 2005.
6. John Berger: "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.
7. Paul Reid, Biometrics for Network Security, Pearson Education, 2004.
8. Nalini K Ratha, Ruud Bolle, Automatic fingerprint Recognition System, Springer, 2003
9. L C Jain, I Hayashi, S B Lee, U Halici, Intelligent Biometric Techniques in Fingerprint and Face Recognition CRC Press, 1999.
10. John Chirillo, Scott Blaul, Implementing Biometric Security, John Wiley, 2003.
11. S.Y. Kung, S.H. Lin, M.W.Mak, Biometric Authentication: A Machine Learning ApproachPrentice Hall, 2005.

IOE 4421 Lightweight Cryptography [3-0-0-3]

Prerequisite for the Course

Student should have a passing Grade in Number Theory and Mathematical Theory of Coding (IMA 312), Discrete Mathematics (IMA 111) or the instructor's approval.

Course Objectives

- To familiarize with the design strategies and mathematic involved in Lightweight Cryptography.
- To analyze various lightweight cryptographic primitives.
- To identify the real time applications of Lightweight cryptography.

Expected Outcome

Students who successfully complete this course will be able to:-

- To understand the design strategies of lightweight ciphers to secure resource constrained devices.
- To compare various lightweight cryptographic algorithms.
- To acquire the fundamental knowledge on the applications of lightweight cryptography

Syllabus

Introduction, Overview of Lightweight Cryptography - Security Threats for resource constrained devices, Design strategies for lightweight cryptography - Constraints and Compromises of Lightweight Algorithms- Modes of Operation

Lightweight Cryptographic Primitives

Lightweight Block Ciphers: DESL and DESXL-PRESENT-CLEFIA - LED-SIMON and SPECK-TWINE-PRINCE-MIDORI-RECTANGLE- GRANULE-CRAFT,

Lightweight Stream Ciphers, Lightweight HASH functions, Lightweight Message Authentication Codes

Key management and Applications of Lightweight Cryptography

Key management: Challenges in Designing IoT Group Key Management Protocols- Lightweight Group Key Management Protocols-Symmetric

Key Constructions- Asymmetric Key Constructions. Applications: IPsec, TLS, Cyber Physical Systems, IoT devices

References

1. Kerry A. McKay Larry Bassham Meltem Sönmez Turan Nicky Mouha, "Report on Lightweight Cryptography" NIST, Computer Security Division Information Technology Laboratory , https://doi.org/10.6028/NIST.IR.8114
2. Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, Yannis Papaefstathiou, "A survey of lightweight stream ciphers for embedded systems" 21 December 2015, https://doi.org/10.1002/sec.1399
3. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A.: PRESENT: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems, CHES 2007, Springer, LNCS, 4727, pp. 450–466 (2007)
4. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Fast Software Encryption (FSE 2007), Springer, LNCS, 4593, pp. 181–195, (2007).
5. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: a new family of lightweight block ciphers. RFID Security and Privacy, Springer, LNCS 7055, 1–18 (2012)
6. Jan Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw, "The LED block cipher", In Proceedings of the 13th international conference on Cryptographic hardware and embedded systems (CHES'11), Bart Preneel and Tsuyoshi Takagi (Eds.). Springer-Verlag, Berlin, Heidelberg, 326-341. (2011)
7. Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2011). Twine: A lightweight, versatile block cipher. In ECRYPT Workshop on Lightweight Cryptography (pp. 146169).
8. Engels, D., Saarinen, M.O., Schweitzer, P., Smith, E.M.: The hummingbird-2 lightweight authenticated encryption algorithm. RFID Security and Privacy, Springer, LNCS 7055, 19–31 (2011)
9. Borghoff, J., et al.: PRINCE A Low-latency Block Cipher for Pervasive Computing Applications. In: Advances in Cryptology ASIACRYPT 2012, Springer, LNCS, 7658, pp. 208–225 (2012)
10. Yibin Dai and Shaozhen Chen, "Cryptanalysis of full PRIDE block cipher", Science China Information Sciences 2014, DOI: 10.1007/s11432-015-5487-3.
11. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalcin, T.: Block Ciphers Focus On The Linear Layer (feat. PRIDE). In: Advances in Cryptology—CRYPTO, Springer, LNCS, vol. 8616, pp. 57–76 (2014)
12. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, Ingrid Verbauwhede. RECTANGLE: A Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms. SCIENCE CHINA Information Sciences, December, 2015, Vol. 58: 122103(15), doi: 10.1007/s11432-015-5459-7
13. Subhadeep Banik and Andrey Bogdanov and Takanori Isobe and Kyoji Shibutani and Harunaga Hiwatari and Toru Akishita and Francesco Regazzoni, "Midori: A Block Cipher for Low Energy", Cryptology ePrint Archive, (2015), https://eprint.iacr.org/2015/1142
14. Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017
15. Bansod, Gaurav et al. "GRANULE: An Ultra lightweight cipher design for embedded security." IACR Cryptology ePrint Archive 2018 (2018): 600.
16. Beierle, C., Leander, G., Moradi, A., & Rasoolzadeh, S, "CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks". IACR Transactions on SymmetricCryptology, pp:5-45,(2019). https://doi.org/10.13154/tosc.v2019.i1.5-45.
17. Andrey Bogdanov,Miroslav Knežević,Gregor Leander,Deniz Toz,Kerem Varıcı,Ingrid Verbauwhede, "SPONGENT: A Lightweight Hash Function" Lecture Notes in Computer Science book series (LNCS, volume 6917)
18. Wu, W., Wu, S., Zhang, L., Zou, J., Dong, L.: Lhash: A lightweight hash function (full version). IACR Cryptology ePrint Archive, 2013:867 (2013)
19. Baraa Tareq Hammad, Norziana Jamil, Mohd Ezanee Rusli and Muhammad Reza Z`aba , "A survey of Lightweight Cryptographic Hash Function" International

Journal of Scientific & Engineering Research Volume 8, Issue 7, July-2017
20. Chowdhury, Amrita & Dasbit, Sipra. (2015). LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network. 1-6. 10.1109/GLOCOM.2015.7417118.
21. BaraaTareq Hammad, Norziana Jamil, Mohd Ezanee Rusli and Muhammad Reza Z`aba , "A survey of Lightweight Cryptographic Hash Function" International Journal of Scientific & Engineering Research Volume 8, Issue 7, July-2017
22. Chowdhury, Amrita &Dasbit, Sipra. (2015). LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network. 1-6. 10.1109/GLOCOM.2015.7417118.
23. Boneh, Dan, Xavier Boyen, and Eu-Jin Goh. "Hierarchical identity-based encryption with Concerns and challenges." Egyptian Informatics Journal (2020). journal on computing 32.3 (2003): 586-615. constant size ciphertext." Annual International Conference on the Theory and Applications of Cryptographie Techniques. Springer, Berlin, Heidelberg, 2005.
24. Armknecht, Frederik, et al. "A Guide to Fully Homomorphic Encryption." IACR Cryptol. ePrint Arch. 2015 (2015): 1192.
25. Wenbo Mao "Modern Cryptography Theory and Practice", Pearson Education, 2004 17.
26. Siddhartha, V., Gaba, G. S., & Kansal, L. "A Lightweight Authentication Protocol using Implicit Certificates for Securing IoT Systems". Procedia Computer Science, 2020. 167, 85– 96. ELSEVIER
27. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review, Security and Communication Networks, 2018, Wiley 1–9.
28. Elahe Fazeldehkordi, Olaf Owe Josef Noll,"Security and Privacy in IoT Systems: A Case Study of Healthcare Products" 13th International Symposium on Medical Information and Communication Technology (ISMICT).