BACHELOR'S DEGREE PROGRAMME

B.Tech.

Computer Science and Engineering with Specialization in Cyber Security

Curricula & Syllabi

Academic Curricula

2024-2028

SCHOOLOFCOMPUTERENGINEERING

KALINGAINSTITUTEOF INDUSTRIAL TECHNOLOGY
BHUBANESWAR – 751024

ODISHA,INDIA

Programme Specific Outcome (PSO)

- Experiment and prepare programming concepts and provide new ideas and innovations towards research and societal issues in the field of cyber security and social network security.
- Analyse and develop secure ways to store, send and process data which is continuously generated in this world of Internet of things and artificial intelligence. Efficient design of varying complexity can be made possible with the help of intrusion detection and prevention system, cryptography, and by providing physical security of IT infrastructure. Finally specify, design, develop, test and maintain usable systems that behave reliably and efficiently.
- Apply standard and advanced security providing algorithms and by using the approach of secure coding-based concepts, practices and strategies in order to develop sustainable products using AI-based technology to deliver a quality product for Business, Education, e-trade, Training and/or E-governance.

Guideline and Notes to obtain the Specialization

A student has to follow the B.Tech Computer Science curricula. To get the specialization the student has to take the following as the professional electives in the respective semester from the basket.

PE: Professional Elective				
PE	**Course Code**	**Course Title**	**Pre-requisites**	**Credits**
PE I		Any subject from the PE I basket of CSE Syllabus		3
PE II		Any subject from the PE II basket of CSE Syllabus	-	3
PE III	CS30034	Principle of Cryptography	MA21002	3
PE IV	CS40017	Network and Cyber Security		3
PE V	CS40012	Block chain		3

Course Title	Principles of Cryptography
Course Code (Credit)	CS 30034(L-T-P-Cr: 3-0-0-3)

Course Objectives:

- To gain knowledge about the mathematics of the cryptographic algorithms
- To get an insight into the working of different existing cryptographic algorithms
- To learn about key exchange protocols and attacks on such protocols
- Tointroducethefundamentalconceptsofhashfunctionsanddigitalsignatures
- To learn how to use cryptographic algorithms in security

Course Contents:

UNIT I

Mathematical Foundations:
NumberTheory:Fermat'stheorem,Cauchy'stheorem,Chineseremaindertheorem,Primalitytestingalgorithm, Euclid'salgorithmforintegers, quadraticresidues, Legendresymbol,Jacobisymbol.*

UNIT II

ClassicalCryptosystems:Cryptographyandcryptanalysis,ClassicalCryptography,differenttypeofattack:
CMA,CPA,CCA,Shannonperfectsecrecy,OTP,Pseudorandombitgenerators, streamciphersandRC4.*

UNIT III

Symmetric Key
ciphers:Blockciphers:Modesofoperation,DESanditsvariants,finitefields(2^n),AES,linearanddifferentialcryptanalysis.*

UNIT IV

Asymmetric Key Ciphers: One-way function, Trap doorone-way function, Public key cryptography, RSA cryptosystem, Diffie-Hellman key exchange algorithm, ElGamalCryptosystem.*

UNITV

Message Authentication: Cryptographic hash functions, secure hash algorithm, Message authentication, digital signature, RSAdigitalsignature.*

*Programming assignments are mandatory.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Identify the relevance of number theory, group, ring, finite fields and modular arithmetic in various contexts of Cryptography

CO2:Assessuseofsymmetriccryptosystem,publickeycryptosystemanddigitalsignaturescheme

CO3: Design and implement cryptographic protocols

CO4: Discuss the security of cryptographic algorithms

CO5: Evaluate the security of a protocol based on security metrics

CO6: Justify the usage of security principles and digital signatures for any application

Textbooks:

1. Stinson.D.,"Cryptography:TheoryandPractice",ThirdEdition,Chapman &Hall/CRC,2012.
2. Douglas Robert Stinson, Maura Paterson. "Cryptography:Theoryand Practice", FourthEdition,Chapman&Hall/CRC,2012.

ReferenceBooks:

1. W.Mao,"ModernCryptography:Theory&Practice",PearsonEducation,2010.
2. William.Stallings,"CryptographyandNetworkSecurityPrinciplesandpractice",SeventhEdition,PearsonEducation,2013.

Course Title	**Network and Cyber Security**
Course Code (Credit)	**CS40017 (L-T-P-Cr: 3-0-0-3)**

Course Objectives:

- To gain knowledge about the cyber security in the real world applications.
- To understand the requirements of security protocols in the networks.
- To learn about the ethics and cyber laws.
- To realize different authentication mechanisms.

Course Contents:

UNIT I

Introduction to Network Security: Introduction to Network security, Model for Network security, Model for Network access security, Real-time Communication Security: Introduction to TCP/IP protocol stack, Implementation layers for security protocols and implications, IPsec: AH and ESP, IPsec: IKE.

UNIT II

Cyber Security: Introduction to cyber security, Media-Based-Vulnerabilities, Network Device Vulnerabilities, Back Doors, Denial of Service (DoS), Spoofing, Man-in-the-Middle, and replay, Protocol-Based Attacks, DNS Attack, DNS Spoofing, DNS Poisoning, ARP Poisoning, TCP/IP Hijacking, Virtual LAN (VLAN), Demilitarization Zone (DMZ) , Network Access Control (NAC), Proxy Server , Honey Pot , Network Intrusion Detection Systems (NIDS) and HostNetwork Intrusion Prevention Systems Protocol Analyzers, Internet Content Filters

UNIT III

Cyber Law and Ethics: Policy vs. Law, Types of Law, General Computer crime laws, U.S. copyright law, U.K. computer security laws, Ethics and education, Codes of ethics of professional organizations.

UNIT IV

Authentication: Kerberos, X.509 Authentication Service, Scanning: Port Scanning, Port Knocking- Advantages, Disadvantages. Peer to Peer security. Electronic Mail Security: Distribution lists, Establishing keys, Privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, anonymity, Pretty Good Privacy (PGP)

UNIT V

Firewalls and Web Security: Packet filters, Application level gateways, Encrypted tunnels, Cookies.

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Distinguish and analyze available network and network layer security such as IPSec

CO2: Analyze and evaluate the cyber security needs of an organization

CO3: Understand various threats and vulnerabilities of a network, and explain appropriate countermeasures

CO4: Illustrate the legal, ethical and professional issues in cyber security

CO5: Understand the authentication in networks and secure mail services

CO6: Justify the usage of firewalls and gateways

Text books:

1. William Stallings, “Cryptography and Network Security Principles and practice”, 8th Edition, Pearson Education, 2023.
2. Michael E. Whitman, Herbert J Mattord, “Principles of Information Security”, Cengage, Seventh Edition, 2023.

Reference Books:

1. Atul Kahate, “Cryptography and Network Security”, 4th edition, McGraw Hill, 2019.
2. Bernard L. Menezes, Ravinder Kumar, “Cryptography, Network Security and Cyber Laws”, 1st edition, cengage, 2018.
3. Charlie Kaufman, Radia Perlman, Mike Speciner, Ray Perlner, “Network Security: Private Communications in a Public World”, 3rd edition, Pearson, 2024.

Course Title	**Block Chain**
CourseCode (Credit)	**CS40012 (L- T- P-Cr: 3-0-0-3)**

Course Objectives

- To understand the design principles Block Chain
- To describe differences between proof-of-work and proof-of-stake consensus
- To understand building a distributed application
- To understand Bitcoin's consensus mechanism

Course Contents:

Unit I

Blockchain Fundamentals:Fundamental of Blockchain Technology and its Importance, Electronic Systems and Trust, Distributed Versus Centralized Versus Decentralized, Bitcoin Predecessors, DigiCash, E-Gold, Cryptographic hash functions, Properties of a hash function-Hash pointer and Merkle tree, digital signatures, B-Money, Evolution of the Blockchain Technology, Storing Data in a Chain of Blocks, Compelling Components, Achieving Consensus

Unit II

Cryptocurrency Fundamentals:Basic cryptocurrency system, Public and Private Keys in Cryptocurrency Systems, The UTXO Model, Transactions, Signing and Validating Transactions, Bitcoin Transaction Security, Wallet Types: Custodial Versus Noncustodial, Lightweight wallets, Hierarchical deterministic wallets, Permissioned and Permissionless Consensus, Proof-of-Work, Proof-of-Stake, Proof of Burn, Proof of Elapsed Time, Bitcoin Miner, Mining Difficulty

Unit III

Distributed Consensus:Permissioned Blockchain: Design issues for Permissioned blockchains, Execute contracts, State machine replication, Overview of Consensus models for permissioned blockchain- Distributed consensus in closed environment, Paxos, RAFT Consensus Algorithm,

Practical Byzantine Fault Tolerance (PBFT), Lamport-Shostak-Pease BFT Algorithm.

Unit IV

Forks and Altchains:Understanding Forks, Contentious Hard Forks, The Bitcoin Cash Fork, Altcoins, Litecoin, Privacy-Focused Crypto-currencies, Segregated witness, Validation and Analysis of Smart Contracts, Evolution of Ethereum, The Ethereum Classic Fork, Comparison among Bitcoin, Ethereum, Stellar, Monero, ZCash, Quorum and Hyperledger fabric. Enterprise, Healthcare and transportation application of Blockchain

Course Outcomes:

Upon completion of this course, the students will be able to:

CO1: Explain the design principles of Bitcoin and Ethereum.

CO2: List and describe differences between proof-of-work and proof-of-stake consensus.

CO3: Interact with a blockchain system by sending and reading transactions

CO4: Design, build and deploy a distributed application.

CO5: Apply the concept of Bitcoin's consensus mechanism and the interaction between Bitcoin and Altcoins

CO6: Familiarize with Ethereum, smart contracts and related technologies, and solidity language

Textbooks:

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
2. Lorne Lantz & Daniel Cawrey, Mastering Blockchain Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications, O'REILLY Publications

Reference Books:

1. Bina Ramamurthy, Blockchain in Action, MANNING Publication.
2. Bikramaditya Singhal, Gautam Dhameja, and PriyansuSekhra Panda, Beginning Blockchain, Apress Publication.
3. Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, "Blockchain Technology: Cryptocurrency and Applications", World cientific, 2020.
4. Josh Thompson, "Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.