श्रद्धावान लभते ज्ञानम्
Good Education, Good Jobs

University of Engineering and Management
Institute of Engineering & Management, Salt Lake Campus
Institute of Engineering & Management, New Town Campus
University of Engineering & Management, Jaipur

श्रद्धावान लभते ज्ञानम्
Good Education, Good Jobs

Minor Degree in Cyber Security

Syllabus for Minor Degree in Cyber Security
for
B.Tech Admission Batch 2023

Minor Degree in "Cyber Security"

		Course Structure					
S. No.	**Course Code**	**Title**	**L**	**T**	**P**	**Credits**	**Semester**
1	CBS-01	Database Security and Access Control	3	0	2	4	6
2	CBS-02	Information Theory for Cyber Security	3	0	2	4	7
3	CBS-03	Steganography and Digital Watermarking	3	0	0	3	7
4	CBS-04	Data Encryption	3	0	2	4	8
5	CBS-05	Security Assessment and Risk Analysis	3	0	0	3	8
		TOTAL	15	0	6	18	

Course Coding Nomenclature:

- CBS denotes that minor degree in "Cyber Security".
- 01, 02, 03, 04, 05 are course in order they have to be taken, if taken in different semesters. Multiple course may also be taken in the same semester (if required).

Course Code	**:**	**CBS-01**
Course Title	:	Database Security and Access Control
Number of Credits	:	4 (L: 3; T: 0; P: 2)
Course Category	:	CBS
Pre-requisites	:	Database Management
Course Objective	:	The objective of the course is to provide fundamentals of database security. Various access control techniques mechanisms were introduced along with application areas of access control techniques.

Course Outcomes:

After completion of course, students will have:

CO1 **To understand and implement classical models and algorithms.**

CO2 **To analyze the data, identify the problems, and choose the relevant models and algorithms to apply.**

CO3 **To assess the strengths and weaknesses of various access control models and to analyze their behaviour.**

Module/ Topic	Sub- Topic	Lecture Hour
1	Introduction to Access Control, Purpose and fundamentals of access control.	7
2	Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control (DAC), Non-Discretionary Access Control, Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations.	8

Module/ Topic	Sub- Topic	Lecture Hour
3	Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access Control policy, Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments.	10

Module/ Topic	Sub- Topic	Lecture Hour
4	Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management. PPS Security techniques- user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals.	8

Module/ Topic	Sub- Topic	Lecture Hour
5	**Cloud Data Security:** Recent trends in Database security and access control mechanisms. **Cloud Data Audit:** Intro, Audit, Best Practice, Key management, Cloud Key Management Audit.	9

Text Books/References:

1. Role Based Access Control: David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli.

Online Resources:

1. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf.
2. https://www.coursera.org/lecture/advancedsystem-security-topics/role-based-access-control-rbac-bYvzS

Course Code	:	**CBS-02**
Course Title	:	**Information Theory for Cyber Security**
Number of Credits	:	4 (L: 3; T: 0; P: 2)
Course Category	:	CBS
Pre-requisites	:	Probability Theory, Computer Networks
Course Objective:	:	The objective of this course is to provide an insight to information coding techniques, error correction mechanism for cyber security.

Course Outcomes:

After completion of course, students would be able:

CO1 **To introduce the principles and applications of information theory.**

CO2 **To justify how information is measured in terms of probability and entropy.**

CO3 **To learn coding schemes, including error correcting codes.**

Course Contents:

Module/ Topic	Sub- Topic	Lecture Hour
1	Shannon's foundation of Information theory, Random variables, Probability distribution factors, Uncertainty/entropy information measures, Leakage, Quantifying Leakage and Partitions, Lower bounds on key size: secrecy, authentication and secret sharing. Provable security, computationally-secure, symmetric cipher.	8

Module/ Topic	Sub- Topic	Lecture Hour
Module 2	Secrecy, Authentication, Secret sharing, Optimistic results on perfect secrecy, Secret key agreement, Unconditional Security, Quantum Cryptography, Randomized Ciphers, Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques.	8

Module/ Topic	Sub- Topic	Lecture Hour
Module 3	Information-theoretic security and cryptograph, basic introduction to Diffie-Hellman, AES, and side-channel attacks.	8
Module 4	Secrecy metrics: strong, weak, semantic security, partial secrecy, Secure source coding: rate-distortion theory for secrecy systems, side information at receivers, Differential privacy, Distributed channel synthesis.	10

Module/ Topic	Sub- Topic	Lecture Hour
Module 5	Digital and network forensics, Public Key Infrastructure, Light weight cryptography, Elliptic Curve Cryptography and applications.	8

Text Books/References:

1. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons.
2. Communication Systems: Analog and digital, Singh and Sapre, Tata McGraw Hill.
3. Fundamentals in information theory and coding, Monica Borda, Springer.
4. Information Theory, Coding and Cryptography R Bose.
5. Multi-media System Design, Prabhat K Andleigh and Kiran Thakrar.

Online resource :

1. https://nptel.ac.in/courses/117101053
2. https://www.coursera.org/learn/information-theory

Online Lab:

Course Code	:	**CBS-03**
Course Title	:	Steganography and Digital Watermarking
Number of Credits	:	3 (L: 3; T: 0; P: 0)
Course Category	:	CBS
Pre-requisites	:	Image and Video Processing, Linear Algebra
Course Objective	:	The objective of course is to provide an insight to steganography techniques. Watermarking techniques along with attacks on data hiding and integrity of data is included in this course.

Course Outcomes:

After completion of course, students will have:

CO1 **Learn the concept of information hiding.**

CO2 **Survey of current techniques of steganography and learn how to detect and extract hidden information.**

CO3 **Learn watermarking techniques and through examples understand the concept.**

Module/ Topic	Sub- Topic	Lecture Hour
1.	**Steganography:** Overview, History, Methods for hiding (text, images, audio, video, speech etc.). **Steganalysis**: Active and Malicious Attackers, Active and passive Steganalysis.	8
2.	Frameworks for secret communication (pure steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive).	8

Module/ Topic	Sub- Topic	Lecture Hour
3.	**Steganography techniques:** Substitution systems, Spatial Domain, transform domain techniques, Spread spectrum, Statistical steganography.	6
4.	**Detection, Distortion, Techniques**: LSB Embedding, LSB Steganalysis using primary sets.	6

Module/ Topic	Sub- Topic	Lecture Hour
5.	**Digital Watermarking**: Introduction, Difference between Watermarking and Steganography, Classification (Characteristics and Applications), types and techniques (Spatial-domain, Frequency-domain, and Vector quantization based watermarking), Watermark security & authentication.	9

Module/ Topic	Sub- Topic	Lecture Hour
6.	Recent trends in Steganography and digital watermarking techniques. Case study of LSB Embedding, LSB Steganalysis using primary sets.	5

Text Books/References:

1. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
3. Information Hiding: Steganography and Watermarking-Attacks and
4. Countermeasures by Neil F. Johnson, Zoran Duric, Sushil Jajodia.
5. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas.

Online Resources:

1. https://swayam.gov.in/nd2_cec20_cs09/preview
2. https://swayam.gov.in/nd2_nou20_cs01/preview

Course Code	:	**CBS-04**
Course Title	:	**Data Encryption**
Number of Credits	:	4 (L: 3; T: 0; P: 2)
Course Category	:	CBS
Pre-requisites	:	Linear Algebra, Cryptography
Course Objective	:	This course will cover the concept of security, types of attack experienced, encryption and authentication for deal with attacks, what is data compression, need and techniques of data compression.

Course Outcomes:

After completion of course, students will have:

CO1 **The knowledge of plain text, cipher text.**

CO2 **The knowledge RSA and other cryptographic algorithm, Key Distribution,**

CO3 **The knowledge of communication model, Various models for data compression.**

Module/ Topic	Sub- Topic	Lecture Hour
1.	**Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attacks. **Encryption Techniques:** Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.	8

Module/ Topic	Sub- Topic	Lecture Hour
2.	**Symmetric & Asymmetric Key Cryptography**: Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.	6

Module/ Topic	Sub- Topic	Lecture Hour
3	**Case Studies of Cryptography:** Denial of service attacks, IP spoofing attacks, Conventional Encryption and Message Confidentiality, Conventional Encryption Algorithms, Key Distribution. **Public Key Cryptography and Message Authentication:** Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management, Firewall.	9

Module/ Topic	Sub- Topic	Lecture Hour
4	**Introduction:** Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification. **Methods of Data Compression:** Data compression-- Loss less & Lossy.	7

Module/ Topic	Sub- Topic	Lecture Hour
5.	**Entropy encoding:** Repetitive character encoding, Run length encoding, Zero/ Blank encoding; Statistical encoding--Huffman, Arithmetic & Lempel-Ziv coding; Source encoding--Vector quantization (Simple vector quantization & with error term).	8
6.	Recent trends in encryption and data compression techniques.	4

Text Books/References:

1. Cryptography and Network Security, Mohammad Amjad, John Wiley & Sons.
2. Cryptography & Network Security by Atul Kahate, TMH.
3. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons.
4. Cryptography and Network Security by B. Forouzan, McGraw-Hill.
5. The Data Compression Book by Nelson, BPB.

Online Resource:

1. https://onlinecourses.nptel.ac.in/noc22_cs90/preview
2. https://www.linkedin.com/learning/learning-cryptography-and-network-security-2

Virtual Lab:

https://cse29-iiith.vlabs.ac.in/

Course Code	**:**	**CBS-05**
Course Title	:	Security Assessment and Risk Analysis
Number of Credits	:	3 (L: 3; T: 0; P: 0)
Course Category	:	CBS
Pre-requisites	:	Computer and Network Security
Course Objective	:	Describe the concepts of risk management in information security. Define and differentiate various Contingency Planning components. Define and be able to discuss incident response options, and design an Incident Response Plan for sustained organizational operations.

Course Outcomes:

After completion of course, students will have:

CO1 **To apply contingency strategies including data backup and recovery and alternate site selection for business resumption planning**

CO2 **To Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.**

CO3 **To Design a Disaster Recovery Plan for sustained organizational operations.**

Module/ Topic	Sub- Topic	Lecture Hour
1	SECURITY BASICS: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security countermeasures-education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.	8

Module/ Topic	Sub- Topic	Lecture Hour
2	**Threats to and Vulnerabilities of Systems:** Threats, major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS). **Countermeasures:** assessments (e.g., surveys, inspections). **Concepts of Risk Management:** consequences (e.g., corrective action, risk assessment), cost/benefit analysis and implementation of controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information).	9

Module/ Topic	Sub- Topic	Lecture Hour
3	**Security Planning:** directives and procedures for policy mechanism. **Contingency Planning/Disaster Recovery:** agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event.	7

Module/ Topic	Sub- Topic	Lecture Hour
4	**Personnel Security Practices and Procedures:** access authorization/verification (needto-know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel. **Auditing and Monitoring:** conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.	8

Module/ Topic	Sub- Topic	Lecture Hour
5.	Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link).	7
6.	Case study of threat and vulnerability assessment.	4

Text Books/References:

1. Information Systems Security, 2ed: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, John Wiley & Sons.
2. Principles of Incident Response and Disaster Recovery, Whitman & Mattord, Course Technology ISBN: 141883663X.

Online Resources:

1. https://swayam.gov.in/nd2_nou20_cs01/preview
2. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf