Model Curriculum for Minor Degree

for UG Degree Courses in Engineering & Technology

(Cyber Security)

2020

ALL INDIA COUNCIL FOR TECHNICAL EDUCATION

Nelson Mandela Marg, Vasant Kunj, New Delhi 110070

www.aicte-india.org

MESSAGE

With a view to enhance the employability skills and impart deep knowledge in emerging areas which are usually not being covered in Undergraduate Degree credit framework, AICTE has come up with the concept of '**Minor Degree**' in emerging areas. The concept of Minor Degree is discussed in the Approval Process Handbook (APH) for the academic session 2020-21 issued by AICTE. Minor Degree will carry 18 to 20 credits in addition to the credits essential for obtaining the Under Graduate Degree in Major Discipline (i.e. 160 credits usually).

Keeping in mind the need of manpower in emerging areas, AICTE with the help of industry-academia experts, has framed the curriculum for seven Minor Degrees:

- Artificial Intelligence and Machine Learning
- Blockchain
- Cyber Security
- Data Science
- Internet of Things (IoT)
- Robotics
- Virtual and Augmented Reality

Courses have been designed after rigorous brainstorming and considering the inputs from the experts of corresponding domain. I am hopeful that knowledge of these emerging areas will help students in capturing the plethora of employment opportunities available in these domains.

I gratefully acknowledge the time and efforts of all those who were involved in preparation of this curriculum especially, the contributions of the members of the Working Group: Prof. Rajesh K. Bhatia from Punjab Engineering College, Prof. Ajay Mittal from Punjab University, Dr. Varun Dutt from IIT Mandi, Ms. Manisha from Education Infosys Ltd, Dr. Shantipal S. Ohol from College of Engineering Pune, Dr. Pushparaj Pathak from IIT Delhi and Dr. S.K Saha from IIT Roorkee. I am very thankful to Prof. Uday. B. Desai, Director, IIT Hyderabad for helping in refining the draft.

The well timed initiative to have this model curriculum addressing the need by Prof. M.P Poonia, Vice Chairman, Prof. Rajive Kumar, Member Secretary, AICTE is highly appreciated. I also appreciate the continuous effort put in coordinating the complete process of development of this curriculum by members of the Policy and Academic Planning Bureau of AICTE namely, Dr. Dileep Malkhede, Adviser–I; Dr. Neeraj Saxena, Adviser-II; Dr. Pradeep Bhaskar, Assistant Director, Mr. Dharmesh Kumar Dewangan & Mr. Rakesh Kumar Pandit, Young Professionals and others.

(Prof. Anil D. Sahasrabudhe)
Chairman
All India Council for Technical Education

Working Group for this Model Curriculum of Minor Degree for UG Degree Courses in Engineering & Technology

S.No	Name	Designation & Organization
1	Prof. Rajesh K Bhatia	Professor, Computer Science and Engineering Dept., Punjab Engineering College (Deemed University)
2	Prof. Ajay Mittal	Professor, Computer Science and Engineering Dept., University Institute of Engineering & Technology, Punjab University
3	Dr. Varun Dutt	Associate Professor, Computer Science and Engineering, IIT Mandi
4	Ms. Manisha	Lead Principal, Education Infosys Ltd.

Working Group for Robotics Model Curriculum:

S.No	Name	Designation & Organization
1	Dr. S.K Saha	Professor, IIT Delhi
2	Dr. Pushparaj Pathak	Professor, IIT Roorkee
3	Prof. S. Ohol	Professor ,College of Engineering Pune,

Cyber Security

Minor Degree in "Cyber Security"

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

Detailed Syllabus

Course Code	:	CBS-01
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 Contents:

Module 1 [8 Lectures]

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.

Module 2 [8 Lectures]

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.

Module 3 [8 Lectures]

Information-theoretic security and cryptograph, basic introduction to Diffie-Hellman, AES, and side-channel attacks.

Module 4 [10 Lectures]

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.

Module 5 [8 Lectures]

Digital and network forensics, Public Key Infrastructure, Light weight cryptography, Elliptic Curve Cryptography and applications.

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. Information Security & Cyber Laws, Gupta & Gupta, Khanna Publishing House.
6. Multi-media System Design, Prabhat K Andleigh and Kiran Thakrar.

Course Outcomes: After completion of course, students would be able:

1. To introduce the principles and applications of information theory.
2. To justify how information is measured in terms of probability and entropy.

3. To learn coding schemes, including error correcting codes.

*****

Course Code	:	CBS-02
Course Title	:	Data Encryption and Compression
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 Contents:

Module 1 [8 Lectures]
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.

Module 2 [6 Lectures]
Symmetric & Asymmetric Key Cryptography: Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.

Module 3 [9 Lectures]
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.

Module 4 [7 Lectures]
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.

Module 5 [8 Lectures]
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).

Module 6 [4 Lectures]
Recent trends in encryption and data compression techniques.

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.
6. Cryptography & Network Security, V.K. Jain, Khanna Publishing House.

Course Outcomes: At the end of this course the student will have the knowledge of plain text, cipher text, RSA and other cryptographic algorithm, Key Distribution, communication model, Various models for data compression.

*****

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 Contents:

Module 1 [8 Lectures]
Steganography: Overview, History, Methods for hiding (text, images, audio, video, speech etc.).
Steganalysis: Active and Malicious Attackers, Active and passive Steganalysis.

Module 2 [8 Lectures]
Frameworks for secret communication (pure steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive).

Module 3 [6 Lectures]
Steganography techniques: Substitution systems, Spatial Domain, transform domain techniques, Spread spectrum, Statistical steganography.

Module 4 [6 Lectures]
Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets.

Module 5 [9 Lectures]
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.

Module 6 [5 Lectures]
Recent trends in Steganography and digital watermarking techniques. Case study of LSB Embedding, LSB Steganalysis using primary sets.

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 Countermeasures by Neil F. Johnson, Zoran Duric, Sushil Jajodia.
4. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas.

Corresponding Online Resources:

1. Cyber Security, https://swayam.gov.in/nd2_cec20_cs09/preview.
2. Introduction to Cyber Security, https://swayam.gov.in/nd2_nou20_cs01/preview

Course Outcomes: After completion of course, students would be able to:

1. Learn the concept of information hiding.
2. Survey of current techniques of steganography and learn how to detect and extract hidden information.
3. Learn watermarking techniques and through examples understand the concept.

*****

Course Code	:	CBS-04
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 Contents:

Module 1 [8 Lectures]

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.

Module 2 [9 Lectures]

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).

Module 3 [7 Lectures]
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.

Module 4 [8 Lectures]
Personnel Security Practices and Procedures: access authorization/verification (need-to-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.

Module 5 [7 Lectures]
Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link).

Module 6 [3 Lectures]
Case study of threat and vulnerability assessment.

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.

Corresponding Online Resources:
1. Introduction to Cyber Security, https://swayam.gov.in/nd2_nou20_cs01/preview
2. (Web Link) http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Course Outcomes: After completion of course, students would be able:
1. To apply contingency strategies including data backup and recovery and alternate site selection for business resumption planning
2. To Skilled to be able to describe the escalation process from incident to disaster in case of security disaster.
3. To Design a Disaster Recovery Plan for sustained organizational operations.

*****

Course Code	:	CBS-05
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 Contents:

Module 1 [7 Lectures]
Introduction to Access Control, Purpose and fundamentals of access control.

Module 2 [8 Lectures]
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.

Module 3 [10 Lectures]
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.

Module 5 [8 Lectures]
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.

Module 6 [9 Lectures]
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.

Text Books/References:

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

Corresponding Online Resources:

1. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf : Smart Card Tutorial.
2. Advanced System Security Topics, https://www.coursera.org/lecture/advanced-system-security-topics/role-based-access-control-rbac-bYvzS.

Course Outcomes:

After completion of this course, the students will be enable:

1. To understand and implement classical models and algorithms.
2. To analyze the data, identify the problems, and choose the relevant models and algorithms to apply.
3. To assess the strengths and weaknesses of various access control models and to analyze their behaviour.

*****