RCOEM

Shri Ramdeobaba College of
Engineering and Management, Nagpur

# SHRI RAMDEOBABA COLLEGE OF ENGINEERING AND MANAGEMENT, NAGPUR – 440013

**An Autonomous College affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra (INDIA)**

## PROGRAMME SCHEME & SYLLABI
## 2023-24

## B. TECH. (CSE-Cyber Security)

# B. Tech. Computer Science and Engineering [2023-24]
# Teaching & Evaluation Scheme [B. Tech CSE-Cyber Security]

## Semester -I

| Sr. No. | Category | Course Code | Course Name | Hours/week | | | Credits | Maximum marks | | | ESE Duration (Hrs) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | L | T | P | | Continuous Evaluation | End Sem Exam | Total | |
| 1. | BSC | CHT1001 | Chemistry of Smart Materials | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 2. | BSC | CHP1001 | Chemistry of Smart Materials Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 3. | BSC | MAT1002 | Calculus | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4. | ESC | CCT1001 | Digital Electronics | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 5. | ESC | CCP1001 | Digital Electronics Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 6. | ESC | CCT1002 | Programming for problem solving | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 7. | ESC | CCP1002 | Programming for problem solving Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 8. | VSEC | CCT1003 | Computer Workshop – I | 1 | 0 | 0 | 1 | 50 | - | 50 | - |
| 9 | VSEC | CCP1003 | Computer Workshop – I Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 10 | HSSM -IKS | HUT1001 | Foundational Literature of Indian Civilization | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 11. | CCA | PET1001 | Sports-Yoga-Recreation | 1 | 0 | 0 | 1 | 50 | - | 50 | - |
| 12. | CCA | PEP1001 | Sports-Yoga-Recreation Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| | | | **TOTAL** | **15** | **0** | **10** | **20** | | | **850** | **-** |

## Semester-II

| Sr. No. | Category | Course Code | Course Name | Hours/week | | | Credits | Maximum marks | | | ESE Duration (Hrs) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | L | T | P | | Continuous Evaluation | End Sem Exam | Total | |
| 1. | BSC | PHT2001 | Introduction to Quantum Computing | 2 | 1 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2. | BSC | PHP2001 | Introduction to Quantum Computing Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 3. | BSC | MAT2002 | Discrete Mathematics | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4. | BSC | MAP2001 | Computational Mathematics Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 5. | BSC | CHT2007 | Bioinformatics | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 6. | ESC | CCT2001 | Object Oriented Programming | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 7. | ESC | CCP2001 | Object Oriented Programming Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 8. | PCC | CCT2002 | Computer Architecture | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 9 | VSEC | CCT2003 | Computer Workshop – II | 1 | 0 | 0 | 1 | 50 | - | 50 | - |
| 10 | VSEC | CCP2003 | Computer Workshop – II Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 11. | AEC | HUT2002 | English for Professional Communication | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 12. | AEC | HUP2002 | English for Professional Communication Lab | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 13. | CCA | HUP0001 | Liberal/Performing Art | 0 | 0 | 2 | 1 | 50 | - | 50 | - |
| 14. | VEC | HUT2004 | Foundation Course in Universal Human Values | 1 | 0 | 0 | 1 | 50 | - | 50 | - |
| | | | **TOTAL** | **16** | **1** | **12** | **23** | - | - | **1000** | **-** |

**List of courses offered under the Basket of Liberal Arts (HUP0001)**

| Course Code | Course Name |
|---|---|
| HUP0001-1 | Fundamentals of Indian Classical Dance: Bharatnatayam |
| HUP0001-2 | Fundamentals of Indian Classical Dance: Kathak |
| HUP0001-3 | Introduction to Digital Photography |
| HUP0001-4 | Introduction to Japanese Language and Culture |
| HUP0001-5 | Art of Theatre |
| HUP0001-6 | Introduction to French Language |
| HUP0001-7 | Introduction to Spanish Language |
| HUP0001-8 | Art of Painting |
| HUP0001-9 | Art of Drawing |
| HUP0001-10 | Nature camp |
| PEP0001-21 | Disaster Management through Adventure Sports |
| PEP0001-22 | Self-defense Essentials and Basics Knowledge of Defense forces |
| CHP0001-31 | Art of Indian traditional cuisine |
| CHP0001-32 | Remedies by Ayurveda |

| **Exit option: Award of UG Certificate in Major with 43 credits and an additional 8 credits.** | | | |
|---|---|---|---|
| **Exit Courses** | | | |
| 1 | Web Designer | Online/ offline certification Course | 8 |
| 2 | IT Support Engineer | | 8 |
| 3 | Certified Programmer (language learned in Sem-1 and/or Sem-2 [C, C++, Java, Python]) | | 8 |

| Semester - III | | | | | | | | Maximum marks | | | ESE Duration (Hrs) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Sr. No. | Category | Course Code | Course Title | L | T | P | Credits | Continuous Evaluation | End Sem Exam | Total | |
| 1 | PCC | CCT3001 | Data Structures | 3 | 1 | 0 | 4 | 50 | 50 | 100 | 3 |
| 2 | PCC | CCP3001 | Data Structures Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 3 | PCC | CCT3002 | Computer Networks | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4 | PCC | CCP3002 | Computer Networks Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 5 | PCC | CCP3003 | Software Lab-I | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 6 | MDM | MAT3003 | Mathematics for Cyber Security | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 7 | OE | IDT2980 | Open Elective - I | 1 | 0 | 0 | 2 | 50 | 50 | 100 | 3 |
| 8 | HSSM | CCP3005 | Idea Lab | 0 | 0 | 4 | 2 | 25 | 25 | 50 | - |
| 9 | PCC | CCT3006 | Cyber Law and Ethics | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 10 | AEC | HUT3001 | Business Communication | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| | | | **TOTAL** | **19** | **1** | **10** | **21** | **-** | | **800** | **-** |

| Semester - IV | | | | | | | | Maximum marks | | | ESE Duration (Hrs) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Sr. No. | Category | Course Code | Course Title | L | T | P | Credits | Continuous Evaluation | End Sem Exam | Total | |
| 1 | PCC | CCT4001 | Operating Systems | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | PCC | CCP4001 | Operating Systems Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 3 | PCC | CCT4002 | Cryptography | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4 | PCC | CCP4002 | Cryptography Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 5 | PCC | CCT4003 | Theory of Computation | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 6 | MDM | MAT4002 | Probability and Queuing Theory | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 7 | OE | IDT2990 | Open Elective - II | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 8 | PCC | CCP4005 | Software Lab-II | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 9 | CEP/FP /ZZ | CCP4006 | Community Engagement Project | 0 | 0 | 4 | 2 | 25 | 25 | 50 | - |
| 10 | HSSM | MBT4001 | Business and Organizational Management | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 11 | VEC | HUT4002 | Environmental Education | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| | | | **TOTAL** | **19** | **0** | **10** | **24** | **-** | **-** | **900** | **-** |

| Exit option: Award of UG Certificate in Major with 88 credits and an additional 8 credits. | | | |
|---|---|---|---|
| Exit Courses | | | |
| 1 | Application Development (Android) | Online/offline certification Course | 8 |
| 2 | Certified Software Engineer (DevOps) | | 8 |
| 3 | Certified Network Defender (CND) – EC - Council | | 8 |

| Semester - V | | | | | | | | Maximum marks | | | ESE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Sr. No.** | **Category** | **Course Code** | **Course Title** | **L** | **T** | **P** | **Credits** | **Continuous Evaluation** | **End Sem Exam** | **Total** | **Duration (Hrs)** |
| 1 | PCC | CCT5001 | Design & Analysis of Algorithms | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | PCC | CCT5002 | Computer Security | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 3 | PCC | CCP5002 | Computer Security Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 4 | PCC | CCT5003 | Basics of Ethical Hacking | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 5 | PCC | CCP5003 | Basics of Ethical Hacking Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 6 | PCC | CCT5004 | Program Elective-1 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 7 | MDM | CCT5005 | Artificial Intelligence and Machine Learning | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 8 | MDM | CCP5005 | Artificial Intelligence and Machine Learning Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 9 | OE | IDT3980 | Open Elective - III | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 2 |
| | | | **TOTAL** | **18** | **0** | **6** | **21** | **-** | **-** | **750** | **-** |

| Semester - VI | | | | | | | | Maximum marks | | | ESE Duration (Hrs) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Sr. No.** | **Category** | **Course Code** | **Course Title** | **L** | **T** | **P** | **Credits** | **Continuous Evaluation** | **End Sem Exam** | **Total** | |
| 1 | PCC | CCT6001 | Introduction to Cloud Security | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | PCC | CCP6001 | Introduction to Cloud Security Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 3 | PCC | CCT6002 | Database Management System | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4 | PCC | CCP6002 | Database Management System Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 5 | PCC | CCT6003 | Software Engineering and Project Management | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 6 | PCC | CCP6003 | Software Engineering and Project Management Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 7 | PCC | CCT6004 | Program Elective-2 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 8 | PCC | CCT6005 | Program Elective-3 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 9 | PCC | CCT6006 | Deep Learning | 2 | 0 | 0 | 2 | 50 | 50 | 100 | 2 |
| 10 | VSEC | CCP6007 | Mini Project | 0 | 0 | 4 | 2 | 25 | 25 | 50 | - |
| **TOTAL** | | | | **17** | **0** | **10** | **22** | | | **800** | |

| **Exit Option: Award of UG Certificate in Major with 131 credits and an additional 8 credits.** | | | |
|---|---|---|---|
| **Exit Courses** | | | |
| 1 | Certified Cloud Engineer (AWS, AZURE) | Online/ offline certification Course | 8 |
| 2 | Certified Cloud Security (ZScaler) | | 8 |
| 3 | Certified Ethical Hacker (EC - Council) | | 8 |

| Semester - VII | | | | | | | | Maximum marks | | | ESE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Sr. No.** | **Category** | **Course Code** | **Course Title** | **L** | **T** | **P** | **Credits** | **Continuous Evaluation** | **End Sem Exam** | **Total** | **Duration (Hrs)** |
| 1 | PCC | CCT7001 | Compiler Design | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | PCC | CCT7002 | Secure Coding | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 3 | PCC | CCT7003 | Network Security Administration | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 4 | PCC | CCP7003 | Network Security Administration Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 5 | PCC | CCT7004 | Program Elective-4 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 6 | PCC | CCP7004 | Program Elective-4 Lab | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 7 | MDM | CCP7005 | Data Visualization Techniques | 0 | 0 | 2 | 1 | 25 | 25 | 50 | - |
| 8 | Project | CCP7006 | Major Project I | 0 | 0 | 8 | 4 | 50 | 50 | 100 | |
| | | | **TOTAL** | **12** | **0** | **14** | **19** | | | **650** | **-** |

| Semester - VIII | | | | | | | | Maximum marks | | | ESE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Sr. No.** | **Category** | **Course Code** | **Course Title** | **L** | **T** | **P** | **Credits** | **Continuous Evaluation** | **End Sem Exam** | **Total** | **Duration (Hrs)** |
| 1 | PEC | CCT8001 | Program Elective-5 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | PEC | CCT8002 | Program Elective-6 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 3 | Project | CCP8003 | Major Project II | 0 | 0 | 12 | 6 | 50 | 50 | 100 | - |
| | | | | | | | **Total** | **150** | **150** | **300** | |
| **OR** | | | | | | | | | | | |
| 1 | PEC | CCT8004 | Research Methodology | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| 2 | Project | CCP8005 | Research Project | 0 | 0 | 12 | 6 | 50 | 50 | 100 | - |
| 3 | PEC | CCT8001 | Program Elective-5 | 3 | 0 | 0 | 3 | 50 | 50 | 100 | 3 |
| | | | | | | | **Total** | **150** | **150** | **300** | |
| **OR** | | | | | | | | | | | |
| 1 | Internship | CCP8006 | Internship / TBI Internship | 0 | 0 | 24 | 12 | 100 | 100 | 200 | |
| | | | **TOTAL** | **0** | **0** | **24** | **12** | | | **200** | **-** |

## Electives Basket:

| Program Elective - 1 | Program Elective - 2 | Program Elective - 3 | Program Elective - 4 | Program Elective - 5 | Program Elective - 6 |
|---|---|---|---|---|---|
| CCT5004 – 1 Operating Systems for Cyber Security | CCT6004 – 1 Wireless & Mobile Device Security | CCT6005 – 1 Managing Risk in Information Systems | CCT7004 – 1 Database & Email Forensics | CCT8001 -1 Vulnerability Assessment and Penetration Testing | CCT8002 – 1 Testing Cyber Crime Investigation and Digital Forensics |
| CCT5004 – 2 Threat and Malware Analysis | CCT6004 – 2 Incident Handling & Response | CCT6005 – 2 IoT Security | CCT7004 – 2 Auditing IT Infrastructure for Compliance | CCT8001- 2 Disaster Recovery & business continuity management | CCT8002 – 2 Executive Governance and Management in IT Security |
| CCT5004 – 3 Security Policies and implementation | CCT6004 – 3 Security Strategies in Windows & Linux | CCT6006 – 3 Application Security | CCT7004 – 3 Blockchain Security | CCT8001 - 3 Mobile Application Security Testing | CCT8002 – 3 Security in Social Networks |

## List of Open Electives:

| Sr. No. | Subject Code | Name of Subject |
|---|---|---|
| Open Elective I | IDT2980 | Cyber Defense Strategies |
| Open Elective II | IDT2990 | Network Security Fundamentals |
| Open Elective III | IDT3980 | Basics of Ethical Hacking |

**Syllabus for Semester VII, B. TECH CSE (Cyber Security)**
**Course Code: CCT7001 Course: Compiler Design**
**L: 3 Hrs T: 0 Hr P: 0 Hr Per Week Total Credits: 3**

---

**Course Prerequisite:** Course on Theory of Computation.

**Course Objectives:**

1. To understand the theory and practice of compiler implementation.
2. To explore the principles, algorithms, and data structures involved in the design and construction of compilers.
3. To understand various phases of compiler and their working.

**Syllabus**

**UNIT-I: Introduction to Compilers**

Introduction to Compilers, Phases of compiler design, Relating Compilation Phases with Formal Systems, Lexical Analysis- Lexical analysis, tokens, pattern and lexemes, Design of Lexical analyzer, Regular Expression, transition diagram, recognition of tokens, Lexical Errors.

**UNIT-II: Syntax Analysis**

Specification of syntax of programming languages using CFG, Top-down parser, design of LL(1) parser, bottom up parsing techniques, LR parsing, Design of SLR, CLR, LALR parsers, Parser Conflicts.

**UNIT-III: Syntax directed translation**

Study of syntax directed definitions & syntax directed translation sche~~me~~s, Type and Type Checking, implementation of SDTS, intermediate notations- postfix, syntax tree, TAC, translation of Assignment Statement, expressions, controls structures, Array reference.

**UNIT-IV: Code optimization**

Machine-independent Optimisation- Local optimization techniques, loop optimization- control flow analysis, data flow analysis, Loop invariant computation, Induction variable removal, other loop optimization techniques, Elimination of Common sub expression, and Machine- dependent Optimisation techniques.

**UNIT-V: Code generation**

Problems in code generation, Simple code generator, code generation using labelling algorithm, Code Generation by Dynamic Programming.

**Storage allocation & Error Handling**

Run time storage administration stack allocation, Activation of Procedures, Storage Allocation Strategies, symbol table management, Error detection and recovery- lexical, syntactic and semantic.

**Course Outcomes:**

After successful completion of the course students will be able to:

1. Implement lexical analyzer from language specification.
2. Realize bottom up and top-down parsers incorporating error handling.
3. Demonstrate syntax directed translation schemes, their implementation for different programming language constructs.
4. Implement different code optimization and code generation techniques using standard data structures.

**Text Books:**


1. Aho, Sethi, and Ullman; Compilers Principles Techniques and Tools; Second Edition, Pearson education, 2008.
2. Alfred V. Aho and Jeffery D. Ullman; Principles of Compiler Design; Narosa Pub.House, 1977.
3. Manoj B Chandak, Khushboo P Khurana; Compiler Design; Universities Press, 2018.


**Reference Books:**


1. Vinu V. Das; Compiler Design using Flex and Yacc; PHI Publication, 2008.
2. V. Raghavan; Principles of Compiler Design, McGraw Hill Education (India), 2010.

**Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCT7002 Course: Secure Coding**
**L: 2 Hrs, T:1Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. To comprehend the fundamentals of Secure coding and its significance.
2. To identify various security attacks on an application
3. To recognize and remove common coding errors that lead to vulnerabilities in an application.
4. To comprehend various secure coding techniques for developing a secureapplication.

**Syllabus**

Unit I Fundamentals of Secure Coding: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Keyloggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Teardrop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security, Vulnerabilities- buffer overflows, Invalidated input, race conditions, access- control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit II Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline

Unit III Threat modeling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defense in Depth and Principle of Least Privilege

Unit IV Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks, Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM.

Unit V Database and Web-specific issues: SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters

Unit VI Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Understand the basics of secure programming
2. Analyze the most frequent programming errors leading to software vulnerabilities
3. Identify security problems in software
4. Comprehend and protect against security threats and software vulnerabilities

5. Apply their knowledge to the construction of secure software systems

**Textbooks**

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press.
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress.
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional.

**Reference Books**

1. Robert C. Seacord, Secure Coding in C and C++, 2nd Edition, Addison-Wesley, 2013
2. CERT C CodingStandard. Available online: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standa rd
3. Wenliang Du, Computer Security – A hands-on Approach, Second Edition, Create space Independent Pub; 2019.

**Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCT7003 Course: Network Security Administration**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. Learn the building blocks of network architecture and its security.
2. Understand the implementation of security controls in an organizational environment.
3. Explore high-level network management tools, techniques & procedures.

**Syllabus**

**Unit I:** Network security overview, benefits of good security practices, 3 Ds of security, business processes vs technical controls, risk analysis and defensemodels, threat vectors, Lollipop model, Onion model, security policy development - developers, audience, organization, topics, policy implementation

**Unit II:** Security organization, separation of duties, security operations management, lifecycle management, enforcement, data classification, documentation, authentication, EAP, authorization, ACLs, data security architecture, securingdata in flight, file encryption, digital rights management

**Unit III:** Security management architecture, AUP, administrative security, accountability controls, activity monitoring and audit, secure network design,wireless impact, remote access considerations, network hardening, anti- spoofing and source routing, logging

**Unit IV:** Types of firewalls, NAT, VPN protocols, SSL VPNs, client/server remote access threats, remote client security, radio frequency security, data-link layer wireless security flaws, wireless network hardening practices

**Unit V:** IDS types and detection models, Wireless IDS, IPS, IDS logging and alerting, IDS deployment considerations, integrity and availability architecture, patching, backups, system and network redundancy, network role-based security, proxy servers, credit card security

**Unit VI:** Disaster recovery, business continuity, malicious mobile code, countermeasures, creating a computer security defense plan, network regulations, Computer Fraud and Abuse Act, unauthorized access to electronic communications, compliance with laws in conducting incident response

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Identify different elements of network security.
2. Understand the management level of security implementation.
3. Implement network security controls to different network segments.
4. Determine network-specific security solutions.
5. Evaluate network security shortcomings and fulfill them.

**Textbooks**

1. Network Security: The Complete Reference by Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg. McGraw-Hill Publishing.

**Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCP7003 Course: Network Security Administration Lab**
**L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 1**

---

**Course Objectives**

1. Implement risk analysis and defense models in networks.
2. Classify, authenticate and authorize different elements of network infrastructure.
3. Generate and implement organization-specific network defense plans.

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Design security processes & policies for network security.
2. Implement authentication and authorization controls in networks.
3. Secure data transmissions and stored data within a network.
4. Implement network perimeter security through firewall, IDS, IPS andVPNs.
5. Comply network security with governing laws and standards.

**Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)**
**Course Code: CCT7004 – 1 Course: Database and Email Forensics**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

---

**Course Objectives**

The objective of this course is to familiarize students with

1. Digital forensics and investigation
2. Database forensics in depth
3. Email Forensics

**Syllabus**

Unit I: Introduction to Digital Forensics – In this module the students will get the basic understanding of what digital forensics is all about and how forensic investigations happen.

Unit II: Why is database forensics important? – In this module the students will learn the emphasis of database forensics and shall analyze the findings as well.

Unit III: Perform forensics on databases – This will be a mix of theory and practical knowledge where the students will learn how to perform forensic investigations on different databases

Unit IV: All about Email – In this module the students shall get in depth knowledge of email systems, clients and servers along with their characteristics.

Unit V: Understanding electronic record management – In this module the students will learn more about the way electronic records are managed in the real time domain.
Understanding email crimes – In this module the students will learn about different case studies about email crimes that have happened in the past and will also learn about the email crime laws.

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Define basics of digital forensics.
2. Describe about databases and the way their forensics are done
3. Interpret how email works and how such crimes are investigated
4. Evaluate the case studies of email crimes and laws that are laid for emailcybercrime.

**Textbooks**

1. Digital Forensics and Incident Response by Gerard Johansen
2. Digital Forensics by Dr. Jeetendra Pande and Dr. Ajay Prasad

**Reference Books**


1. Expert witness- Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Expert_witness 208
2. Expert witness, http://einvestigations.com/computer-forensics/expert-witness/
3. Information Technology Act, 2000 - Wikipedia, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
4. Legal aspects of computing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Legal_aspects_of_computing

**Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)**

**Course Code: CCP7004 – 1 Course: Database & Email Forensics Lab**

**L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01**

---

**Course Objectives**

1. To implement database security practices for solving problems.
2. To implement email parsing systems.
3. To learn the role of forensics in Email & Database security incident handling

**Syllabus**

Experiments based on CCT7004 – 1

**Course Outcome**

On successful completion of the course, students will be able to:

1. Implement various database security practices
2. Implement database forensic techniques
3. Apply email parsing algorithms for email forensics
4. Analyse the case studies of email crimes and laws that are laid for email cybercrime

**Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)**
**Course Code: CCT7004 – 2 Course: Auditing IT Infrastructure for Compliance**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. Learn about the importance of information security auditing and different auditing standards.
2. Understand audit scoping and perform standard-specific security audits in different types of organizations.
3. Explore higher level security governance concepts like CMMI, Quality Assurance etc.

**Syllabus**

Unit I: Introduction to COBIT, Using COBIT to Assess Internal Controls, COBIT Assurance Framework Guidance, ISACA IT Auditing Standards Overview, Risk Management Fundamentals, Quantitative Risk Analysis Techniques, IT Audit Risk and COSO ERM, Performing Effective IT Audits

Unit II: General Controls in Today's IT Environments, ITIL Service Management Best Practices, Systems Software and IT Operations General Controls, Evolving Control Issues: Wireless Networks, Cloud Computing, and Virtualization

Unit III: IT Application Control Elements, Selecting Applications for IT Audit Reviews, Auditing Applications under Development, Application Review Case Study: Client-Server Budgeting System, Importance of Reviewing IT Application Controls, Micro Project - IT Application Auditing

Unit IV: Software Engineering Concepts, CMMI: Capability Maturity Model for Integration, IT Audit, Internal Control, and CMMI, IT Auditing in SOA Environments, Computer-Assisted Audit Tools and Techniques (CAATTs)

Unit V: IT Controls and the Audit Committee, Role of the Audit Committee for IT Auditors, Audit Committee Review and Action on Significant IT Audit Findings, Compliance with IT-Related Laws and Regulations, Understanding and Reviewing Compliance with ISO Standards, Controls to Establish an Effective IT Security Environment

Unit VI: Auditing Telecommunications and IT Communications Networks, Building an Effective IT Internal Audit Function, Quality Assurance Auditing and ASQ Standards, Live Project - IT Security Auditing

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Understand and identify different information security audit standards and frameworks.
2. Differentiate between the compliance requirements of different audit frameworks.
3. Carry out standard IT auditing procedures in organizations.
4. Perform analysis on audit findings and calculate cyber risk.
5. Generate quality audit reports and effectively communicate them to organizations.

**Textbooks**

1. IT Audit, Control, and Security by Robert R. Moeller. Wiley Publishing.

**Reference Books**

1. Auditing Information and Cyber Security Governance – A Controls-Based Approachby Robert E. Davis|2021 Edition. CRC Press.

**Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)**

**Course Code: CCP7004 – 2 Course: Auditing IT Infrastructure for Compliance Lab**

**L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 1**

---

**Course Objectives**

1. Apply different auditing standards as per organization's requirement.
2. Design audit scope and conduct industry-standard audits.
3. Implement security governance through CMMI, quality assurance etc.

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Design audit checklists based on different auditing standards.
2. Scope out necessary elements of auditing.
3. Conduct Information Security audits at organization level.
4. Analyze audit findings and generate remediations and conclusion.
5. Design standardized and detailed audit reports.

**Syllabus for Semester VII, B. Tech. (Computer Science & Engineering) (Cyber Security)**
**Course Code: CCT7004 – 3 Course: Blockchain Security**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. This course aims to provide a survey on blockchain and the topics around such as history of blockchain, cryptography it uses, Bitcoin and other currencies, consensus algorithms, smart contracts, Ethereum, scalability and various use cases.

Syllabus

**Unit I: Blockchain Introduction:** Blockchain Technology Mechanisms & Networks, Blockchain Origins, Blockchain Objectives, Blockchain Users & Adoption, Blockchain Challenges, P2P Systems, Hash Pointers and Data Structures, Blockchain Transactions

**Unit II: Consensus Mechanism:** ermissioned Blockchain, Permisionless Blockchain, Different Consensus Mechanism- Proof of Work, Proof of Stake, Proof of Activity, Proof of Burn, Proof of Elapsed Time, Proof of Authority, Proof of Importance.

**Unit III: Cryptography Fundamentals:** Encryption, Digital Signatures, Public-Key Cryptography, Private Key Cryptography, Distributed Denial-of-Service (DDoS) Attack, 51% Attack, Double spending problem, Merkel Tree, Security Threats to Blockchain Technology

**Unit IV: Crypto currency and Wallet:** Types of Wallet, Desktop Wallet, App based Wallet, Browser based wallet, Metamask, Creating a account in Metamask, Use of faucet to fund wallet, transfer of cryptocurrency in metamask.

**Unit V: Smart contract and Ethereum** Overview of Ethereum, Writing Smart Contract in Solidity, Remix IDE , Different networks of ethereum, understanding blocks in blockchain, compilation and deployment of smart contracts in Remix

**Unit VI: Use Cases:** Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Block chain enabled Trade, We Trade – Trade Finance Network, Supply Chain Financing, Identity on Block chain, Blockchain in energy sector, Blockchain in governance

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Realize the importance of blockchain technology and consensus mechanism
2. Identifying the security risks and challenges associated with blockchain technology
3. Implement browser-based wallets and smart contracts in Remix IDE
4. Recognize the importance of blockchain security in various enterprise applications.

**Text Books**

1. Mastering Blockchain: Third Edition by Imran Bashier, Packt Publishing, 2020, ISBN: 9781839213199,

**Reference Books**

1. Blockchain: Blueprint for a New Economy by Melanie Swan, Oreilly Publication
2. Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood
3. Bitcoin and Cryptocurrency Technologies (Princeton textbook) by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder

**Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)**

**Course Code: CCP7004-3 Course: Blockchain Security Lab**

**L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01**

---

**Course Objectives**

This course aims to provide hands-on experience with blockchain development tools and frameworks, and will be able to use them to build and test their own blockchain projects.

**Syllabus:**

Experiments based on the above syllabus CCT401-3

**Course Outcome:**

On completion of the course the student will be able to

1. Realize different blockchain tools and framework
2. Implement smart contracts for the development of enterprise applications
3. Apply different wallets for the deployments of smart contracts
4. Analyze blockchain security in various enterprise applications

**Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)**

**Course Code: CCP7005 Course: Data Visualization Techniques**

**L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01**

---

**Course Objectives**

1. To introduce advanced tools and libraries for creating interactive and dynamic visualizations.
2. To apply cognitive and perceptual principles to the design of complex data dashboards.
3. To develop skills in transforming multi-dimensional data into meaningful visual stories for stakeholders.

**Syllabus**

- **Module I: Advanced Python/R Visualization:** Mastery of specialized libraries (Seaborn, Plotly, Plotnine) for multi-variate data and high-dimensional aesthetics.
- **Module II: Interactive Visuals & Web Frameworks:** Introduction to building web-based interactive charts using Bokeh, Dash, or Streamlit.
- **Module III: Geospatial and Temporal Mapping:** Visualizing data with geographical components using Folium, Geopandas, or Leaflet.
- **Module IV: Dashboarding & Business Intelligence:** Design and development of professional dashboards using industry tools like Tableau, Power BI, or Google Data Studio.
- **Module V: Data Storytelling:** Techniques for creating author-driven and reader-driven narratives with emphasis on annotations and highlighting.

**List of Practicals**

1. **Multi-variate Analysis:** Create a matrix of visualizations (Facet Grids/Pair Plots) to explore correlations in a high-dimensional dataset.
2. **Interactive Distributions:** Design an interactive histogram and box-plot set that allows users to filter data by categories using **Plotly**.
3. **Geospatial Visualization:** Create a Choropleth map to visualize regional statistics (e.g., COVID-19 cases or Sales by state) using **Folium**.
4. **Network Graphing:** Visualize a social network or a relationship dataset using **NetworkX** or **Gephi** to identify clusters and influencers.
5. **Interactive Time-Series:** Build a time-series dashboard with "range sliders" and "selectors" to analyze trends over a decade.
6. **Hierarchical Data:** Implement a Treemap or Sunburst chart to represent nested categories (e.g., Product Hierarchy or File Systems).
7. **Web-based Dashboard (Part 1):** Develop a single-page interactive data app using **Streamlit** that takes user input to update charts in real-time.
8. **Web-based Dashboard (Part 2):** Deploy a multi-page dashboard with **Dash/Plotly** incorporating data tables and download features.
9. **Business Intelligence Case Study:** Create a sales performance dashboard in **Tableau/Power BI** featuring KPIs, Gauges, and Drill-down charts.
10. **Visualizing Uncertainty:** Create a plot representing error bars, confidence intervals, and probability distributions for a predictive model.
11. **Final Project: Data Story:** Develop a comprehensive "Data Story" on a public dataset (e.g., Kaggle/UCI) using an interactive notebook or dashboard, adhering to best practices of perception.

**Course Outcomes:**

On successful completion of the course, students will be able to:

- **CO1:** Use advanced visualization libraries to preprocess and map complex data onto appropriate visual aesthetics.
- **CO2:** Analyze multi-dimensional datasets to discover hidden patterns and choose the most effective visualization technique for specific data types.
- **CO3:** Evaluate visual representations based on principles of human perception, cognitive load, and design best practices to ensure clarity and accuracy.
- **CO4:** Design and deploy interactive, web-based dashboards and visual stories that facilitate data-driven decision-making for end-users.

**Text Books**


1. Claus O. Wilke, *"Fundamentals of Data Visualization – A Primer on Making Informative and Compelling Figures"*, O'Reilly, 2019.
2. Cole Nussbaumer Knaflic, *"Storytelling with Data: A Data Visualization Guide for Business Professionals"*, Wiley, 2015.
3. Kyran Dale, *"Data Visualization with Python and JavaScript"*, 2nd Edition, O'Reilly, 2022.


**Reference Books**


1. Edward Tufte, *"The Visual Display of Quantitative Information"*, 2nd Edition, Graphics Press, 2001.
2. Tamara Munzner, *"Visualization Analysis and Design"*, AK Peters Visualization Series, CRC Press, 2014.
3. Scott Murray, *"Interactive Data Visualization for the Web: An Introduction to Designing with D3"*, O'Reilly, 2017.

**Syllabus for Semester VIII, B. E. Cyber Security (Computer Science & Engineering)**
**Course Code: CCT8001 -1 Course: Vulnerability Assessment and Penetration Testing**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. Learn about various hacking concepts and requirements of setting-up a penetration testing lab.
2. Learn to use Kali Linux and different penetration testing tools.
3. Explore advanced penetration testing concepts.

**Syllabus**

**Unit I:** Setting up virtual lab, Configuring the Network for Your Virtual Machine, Setting Up Android Emulators, Target Virtual Machines, Setting a Static IP Address, Setting up external servers, Using Kali Linux, Programming

**Unit II:** Tools of the trade, Using Metasploit Framework, Types of Shells, Msfcli, Creating standalone payloads, Information gathering, Red team recon, Finding Vulnerabilities, Capturing Traffic

**Unit III:** Exploitation, Exploiting WebDAV default credentials, Exploiting Open phpMyAdmin, Exploiting Third-party Web Applications, Exploiting NFS shares, Password attacks, Client-side exploitation - Browser, PDF, Java etc.

**Unit IV:** Social engineering, Mass email attacks, Multipronged attacks, Compromising the network, Bypassing anti-virus applications, Post exploitation, Privilege escalation, Lateral movement, Pivoting, Persistence

**Unit V:** Web application testing, Using BurpSuite, SQL injection, XPath injection, LFI, RFI, CSRF, XSS, Wireless attacks, Physical attacks, Stack-based buffer overflowin linux and windows, Known vulnerability in War-FTP, Locating & controlling EIP**.**
Structured exception handler overwrites, Finding attack string in memory, Using a short jump, Fuzzing, Finding bugs with code review, Porting exploits, Replacing shellcode, Writing Metasploit modules, Exploitation mitigation techniques

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Apply penetration testing concepts to network and applications.
2. Identify vulnerabilities in target technology and exploit them.
3. Carry out privilege escalation activities in breached networks.
4. Implement social engineering and physical attacking methods for penetration testing.
5. Design custom hacking scripts.

**Textbooks**


1. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman|2014 Edition. No Starch Press.
2. The Hacker Playbook 3: Practical Guide to Penetration Testing by Peter Kim

**Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCT8001- 2 Course: Disaster Recovery and Business Continuity Management**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. Understand the concept of business continuity
2. Learn the importance of a BCP (business continuity planning)
3. See how load balancing maintains business continuity
4. Know the details of DCP (Disaster recovery plan)
5. Learn how to choose the right fail over solution

**Syllabus**

Unit I:

Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR)-Terms and definitions, BCP under a Governance and BCP Policy making Project Scope and Planning,

Unit II:

Business Organization Analysis, BCP Team Selection, Resource Requirements, Legal and Regulatory Requirements, Business Impact Analysis

Unit III:

Concepts of threat, vulnerabilities, and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting -Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting

Unit IV:

IT recovery strategy, Business continuity strategy development framework - Cost- benefit assessment - Site assessment and selection - Selection of recovery options -Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies

-Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools.

Unit V:

Database recovery - Recovery Plan Development, Personnel Notification, DR site- concepts and management, Backups and Offsite Storage, Backup Media Formats, Software Escrow Arrangements, External Communications, Utilities Logistics and Supplies, Emergency Handling for Crisis Management, safety and rescue of personnel in emergency

Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits. Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Road map - Disaster Recovery Plan (DRP)preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair, ISMS policies, ISO 27000

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Identify the integral aspects of Business Continuity Management
2. Analyze common organizational risks and threats to business system continuity
3. Evaluate an organization's ability to recover from a given disaster or event
4. Apply business continuity and disaster recovery principles to enhance abusiness continuity plan

**Textbooks**

1. Disaster Recovery Handbook –M Wallace and Lawrence Webber , AMACOM; 3rd edition (22 March 2018)
2. Disaster Recovery Planning-S.S.Kambhmmettu

**Reference Books**

1. CISSP handbook

**Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCT8001-3 Course: Mobile Application Security Testing**
**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

**Course Objectives**

1. Learn about various types of mobile application development platforms.
2. Learn to use different mobile app penetration testing tools and frameworks.
3. Explore mobile application security concepts.

**Syllabus**

Unit I: Evolution of mobile apps, Mobile app security, OWASP mobile security project, Mobile security tools, Analyzing iOS Applications, Understanding the Security Model, Understanding iOS Applications, Jailbreaking Explained, Understanding the Data Protection API, Understanding the iOS Keychain, Understanding Touch ID, Reverse Engineering iOS Binaries

Unit II: Analyzing Android applications, Understanding security model, Reverse engineering applications, Attacking Android applications, Accessing storage and login, misusing insecure communications, Tools: Xposed framework, Cydia substrate

Unit III: Identifying and exploiting android implementation issues, reviewing pre- installed apps, Exploiting devices, Infiltrating user data, Writing secure android applications, Principle of least exposure, Storing files securely, Securing WebViews, Logging

Unit IV: Analyzing Windows Phone Applications, Understanding the Security Model, Understanding Windows Phone 8.x Applications, Building a test environment, Analyzing application binaries, Attacking Windows Phone Applications, Attacking Transport Security, Identifying Interprocess Communication Vulnerabilities, Patching .NET Assemblies

Unit V: Identifying windows phone implementation issues, Identifying Insecure Application Settings Storage, Identifying Data Leaks, Identifying Insecure Data Storage, Insecure Random Number Generation, Insecure Cryptography and Password Use, Writing Secure Windows Phone Applications, Storing and Encrypting Data Securely, Securing Data in Memory and Wiping Memory, Secure XML Parsing, Avoiding Native Code Bugs
Analyzing BlackBerry Applications, Understanding BlackBerry Legacy, Understanding the BlackBerry 10 Security Model, BlackBerry 10 Jailbreaking, Using Developer Mode, The BlackBerry 10 Device Simulator, Accessing App Data from a Device, Accessing BAR Files, Attacking BlackBerry Applications, Traversing Trust Boundaries

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Understand different mobile app development operating systems.
2. Identify vulnerabilities in android, windows, blackberry and iOS phones.
3. Reverse engineer mobile apps on multiple platforms.
4. Set up mobile app security testing labs for different operating systems.
5. Secure mobile apps.

**Textbooks**

1. The Mobile Application Hacker’s Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley and Ollie Whitehouse. Wiley Publishing.

**Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)**
**Course Code: CCT8002 – 1 Course: Testing Cyber Crime Investigation and Digital Forensics**
**L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 04**

---

**Course Objectives**

The objective of this course is to familiarize students with

1. Different Cyber laws
2. Types of cyber crimes
3. The way investigations are done

**Syllabus**

Unit I

Introduction to Cyber Laws – In this module the students will get the basic understanding all the cyber laws that are currently in effect.

Unit II Types of cybercrimes – In this module the students will learn the different types of cybercrimes along with analysis on different case studies.

Unit III Social Media Investigation – This module will be a detailed case study analysis module which will focus on different social media crimes and the way they are investigated.

Unit IV Communication Device Based Investigation– In this module the students shall get in depth knowledge of introduction to the communication devices, knowledge on laws related to interception, knowledge on CDR, CDR formats, CDR analysis and investigations on VOIP communications using case studies.

Unit V Mobile Forensics – In this module the students will learn about the introduction to mobile forensics, types of memories on mobile phones, techniques of mobile forensics and the investigation process.

Unit VI Investigation on Financial Frauds and Cybercrime– In this module the students will learn about Introduction to investigation of financial frauds and cybercrime, steps to follow in case of financial frauds, Investigation on ATM withdrawal frauds, online transaction frauds, bank to bank transfer frauds and about the indicative notice under 91 CrPC issued to the banks.

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Define types of cyber laws.
2. Evaluate about types of cybercrimes pertaining in today's cyber society.
3. Describe how investigations are done based on the case studies

**Textbooks**

1. Combating Cyber Crimes by National Center for Justice and the Rule of Law
2. National Cyber crime reference handbook by National Cyber Safety and Security Standards, Ministry of Defence, Ministry of Electronics and Information Technology and

**Reference Books**

1. https://www.ojp.gov/pdffiles1/nij/187736.pdf
2. https://cc.iittp.ac.in/pdfs/Doc%202%20National%20Cyber%20Crime%20Reference%20Handbook%20III%20Edition.pdf

**Syllabus for Semester VIII, B. E. (Computer Science & Engineering)**
**Course Code: CCT8002 – 2 Course: Executive Governance and Management in IT Security**
**L: 3 Hrs, T: 0 Hrs, P: 0 Hrs, Per Week Total Credits: 03**

---

**Course Objectives**

1. To understand formation of an organization wide information security strategy
2. To study approach behind interactions between the C-Suite of the company.
3. To know how to manage risks at an acceptable level
4. To critique creation of information security policies

**Syllabus**

Unit I: Information Security Strategy: Evolution of Information Security, Organization Historical Perspective, Understand the External Environment, The Internal Company Culture, Prior Security Incidents, Audits, Security Strategy Development Techniques

Unit II: Security Management Organization Structure: Relevance of Security Leadership Roles, Security Leader Titles, Techie versus Leader, The Security Leaders Library, Security Leadership Defined, Security Leader Soft Skills, Security Functions

Unit III: Managing the Risk: Accepting Organizational Risk, Risk Ownership Management, Qualitative vs Quantitative Risk Analysis, Risk Management Process, Risk Mitigation Options

Unit IV: Creation of Information Security Policies: Importance of Information Security Policies, Canned Security Policies, Policies, Standards, Guidelines Definitions, Approach for Developing Information Security Policies, Policy Review Process

Unit V: Security Compliance & Control Frameworks: Security Control Frameworks and Standard Examples, Existence of Standards, Integration of Standards and Control Frameworks, Auditing Compliance, Adoption Rate of Standards, The Standards/Framework Value Proposition Security Controls & Incidents.
Managerial Controls, Technical Controls, Operational Controls, Anatomy of an Audit, Audit Execution Phase, Effective Security Communication, Security Incidents & Handling, The Law and Information Security

**Course Outcomes:**

On successful completion of the course, students will be able to:

1. Use enterprise information security practices and various strategies.
2. Apply information security risk evaluation processes for modeling and solving real- world problems.
3. Analyze the impact of different information security policies in enterprise scenarios.
4. Estimate the value propositions of the information security frameworks.

**Textbooks**

1. Information Security Governance Simplified, Todd Fitzgerald, CRC Press

**Reference Books**

1. Enterprise Security: A Data-Centric Approach to Securing the Enterprise, Aaron Woody, Packt Publishing

**Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)**

**Course Code: CCT8002 – 3 Course: Security in Social Networks**

**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

---

**Course Objectives**

1. s

**SYLLABUS**

UNIT – I: Networks and Society

Network preliminaries; Social Networks: Introduction and Applications; Overview of Social Network Analysis; Social Media Content and Levels of Network Analysis.

Networks and Graphs: Types of Networks; Representation of Networks; Network Properties.

UNIT – II: Network Measures

Node Centrality: Degree, Closeness, Betweenness, Edge Betweenness, Katz, Eigen Vector Centrality; Edge and Flow Betweenness; PageRank; Hub and Authority.

Associativity, Transitivity and Reciprocity; Similarity: Structural and Regular Equivalence; Degeneracy: k-Core, Coreness, Core Periphery.

UNIT – III: Network Growth Models and Community Detection

Properties of Real-World Networks: Small World Property, Scale Free Property; Random Network Model; Ring Lattice Network Model; Preferential Attachment Model; Price's Model; Six Degrees of Separation. Types of Communities; Community Detection Methods: Disjoint Community Detection, Overlapping Community Detection, Local Community Detection; Community Detection versus Community Search; Community Evaluation.

UNIT – IV: Ego Networks and Information Diffusion

Ego Network – Overview and Characteristics; Ego Network Measures: Structural Holes, Density, Brokerage. Information Diffusion Overview; Explicit Networks: Herd Behavior, InformationCascades; Implicit Networks: Epidemical Models, Diffusion of Innovation.

UNIT – V: Security Challenges in Social Networking

The dark side of OSNs and Media; User responses; Opportunities in OSNs; Taxonomy of OSN attacks; Taxonomy of OSN solutions; Malware attacks and Phishing attacks in OSNs.

UNIT – VI: Threats and Preventive Measures in OSNs

Attackers and Social Media Platforms; Social media attacks based on account types; Cyber security tools for protecting user accounts. Identity theft and cyber bullying in OSNs.

General practices to protect – system, accounts and information; Issues and challenges in existing security solutions; principles to protect user account on social platform.

**Course Outcomes:**

On completion of the course the student will be able to

1. Analyze network data and complex graphs structures.
2. Apply the basics of social network analysis at various levels.
3. Model various interactions between individuals and actors.
4. Analyze the impact of different attacks on OSNs.

**Textbooks and References:**

1. Tanmoy Chakraborty; Social Network Analysis; First Edition; Wiley India; 2021.
2. Niyati Aggarwal and Adarsh Anand; Social Networks: Modeling and Analysis;CRC Press; 2022.
3. Brij B. Gupta and Somya Ranjan Sahoo; Online Social Network Security: Principles, Algorithms, Applications and Perspectives; CRC Press; 2021.

**References:**

1. David Easley and Jon Kleinberg; Networks, Crowds, and Markets: Reasoning about a Highly Connected World; Cambridge University Press; 2001.
2. Michael Cross; Social Media Security: Leveraging Social Networking while Mitigating Risk; Elsevier Science; 2013.
3. Stanley Wasserman and Katherine Faust; Social Network Analysis: Methods and Applications; Cambridge University Press; 1994.
4. Carl Tim and Richard Perez; Seven Deadliest Social Network Attacks; Elsevier Science; 2010

**Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)**

**Course Code: CCT8004 Course: Research Methodology**

**L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03**

---

**Course Outcomes**

1. Ability to critically evaluate current research and propose possible alternate directions for further
2. work.
3. Ability to develop hypothesis and methodology for research
4. Ability to comprehend and deal with complex research issues in order to communicate their
5. scientific results clearly for peer review.

**Syllabus**

**Introduction to research methodology**: Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, research Methods versus Methodology, Research and Scientific Method, Research Process, Criteria of good Research, Necessity and Techniques of Defining the Problem, Meaning and need of Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Design, Research ethics, Stress management.

**Literature review, Data collection and sampling design**: Review concepts and theory, review previous findings, Sources of data: Primary and secondary data, Methods of data collection, Sampling fundamentals

**Modelling and Analysis**: Probability distributions, Processing and analysis of data, Data analysis skills, Distributions, Statistical and multivariate analysis, Correlation and regression, Fundamentals of Time series analysis, spectral analysis, Error analysis, Simulation techniques

**Algorithmic processes in Computer science research domains**: Soft computing, Artificial intelligence, NLP, Image processing, Data management techniques, Networks and security, Software systems

**Research Reports**: Structure and components of Research report, Types of report, Layout of research report, Mechanisms and tools for writing research report, LaTeX

**Text and Reference Books**


1. C. R. Kothari, Research Methodology Methods and Techniques, 2nd revised edition, New Age.
2. Richard I Levinamp; DavidS.Rubin,StatisticsforManagement,7/e.PearsonEducation,2005.
3. DonaldR.Cooper,PamelaS.Schindler,BusinessResearchMethods,8/e,TataMcGraw - HillCo. Ltd., 2006.
4. Bendat and Piersol, Random data: Analysis and Measurement Procedures, Wiley Interscience,
5. 2001.
6. Shumway and Stoffer, Time Series Analysis and its Applications, Springer, 2000.
7. Jenkins, G. M., and Watts, D.G., Spectral Analysis and itsApplications,HoldenDay,1986.