PRESERVING AND RECOVERING DIGITAL EVIDENCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Number of Lecture Hours/Week</th>
<th>Exam Marks</th>
<th>Total Number of Lecture Hours</th>
<th>Exam Hours</th>
<th>CREDITS – 04</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SFC21</td>
<td>20</td>
<td>04</td>
<td>80</td>
<td>50</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Course objectives: This course will enable students to
- Different laws related to computer crime
- How to Secure Digital Evidences
- To Understand Investigation Process

Module 1
Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.

Module 2
Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices.

Module 3
Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.

Module 4
Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.

Module 5
Handling the digital crime scene, digital evidence examination guidelines.

Course Outcomes
The students should be able to:
- Explain Digital evidence and computer crime and Laws
- Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems
- Illustrate the Networks basics for digital investigators
- Able to Investigating computer intrusions and cyber stalking
- Explain the basic concepts how to Handling the digital crime scene, digital evidence examination guidelines

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

Reference Books:
OPERATING SYSTEM SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>16SFC22</th>
<th>Exam Marks</th>
<th>80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>04</td>
<td>Exam Hours</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CREDITS – 04

**Course objectives:** This course will enable students to

- Define fundamental concepts and mechanisms for enforcing security in OS.
- Build a secure OS by exploring the early work in OS.
- Illustrate formal security goals and variety of security models proposed for development of secure operating systems.
- Explain architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Analyze variety of approaches applied to the development & extension services for securing operating systems.

**Module 1**

**Introduction:** Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson’s Access Matrix, Mandatory protection system.

**Module 2**

**Multics:** Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

**Module 3**

**Security in ordinary operating system:** UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

**Module 4**

**Security Kernels:** The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era-IX, domain and type enforcement.

**Module 5**

**Case study:** Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration.

**Case study:** Building secure OS for Linux: Linux security modules, security enhanced Linux.

**Course Outcomes**

The students should be able to:
• Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
• Analyze how to build a secure OS by exploring the early work in OS.
• Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
• Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS’s.
• Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

Reference Books:
1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition

SECURED PROGRAMMING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Exam Marks</th>
<th>Exam Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>14SFC23</td>
<td></td>
<td>80</td>
<td>0</td>
</tr>
</tbody>
</table>

CREDITS – 04

Course objectives: This course will enable students to

• Explain the basics of secure programming.
• Demonstrate the most frequent programming errors leading to software vulnerabilities.
• Identify and analyze security problems in software
• Illustrate how to protect against security threats and software vulnerabilities

Module 1
Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks.

Module 2
Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using
correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data.

Module 3

Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision.

Module 4

Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc.

Module 5

I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files.

Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors.

Course Outcomes

The students should be able to:

- How to respond to security alerts which identifies software issues
- Identify possible security programming errors
- Define methodology for security testing and use appropriate tools in its implementation
- Apply new security-enhanced programming models and tools

Question paper pattern:
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books


Reference Books:

CYBER LAWS AND ETHICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016-2017)
SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Exam Marks</th>
<th>Total Lecture Hours</th>
<th>Exam Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>14SFC24</td>
<td>20</td>
<td>80</td>
<td>50</td>
<td>3</td>
</tr>
</tbody>
</table>

CREDITS – 04

Course objectives: This course will enable students to

- Explain the Types of contract law, Digital signature and related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues
- Explain cyber crime investigation and prosecution in depth.

Module 1

Module 2

Module 3
Intellectual Property Law for Cyber Space: Concept of Virtual assets, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.

Module 4
Intellectual Property Law for Cyber Space: Concept of Virtual assets, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.

Module 5
Course Outcomes
The students should be able to:

- Classify the Types of contract law, Digital signature, related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues.
- Interpret the cyber crime investigation and prosecution in depth.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

Reference Books:

BIOMETRIC SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Exam Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>14SFC251</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>03</td>
<td>Exam Hours</td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>40</td>
<td>3</td>
</tr>
</tbody>
</table>

CREDITS – 03

Course objectives: This course will enable students to

- Explain the principles used in biometrics algorithms and systems and most important biometric approaches.
- Illustrate the capability to select a suitable algorithm / system for a given application context (e.g. physical access control)
- Demonstrate a good understanding of the complex relationships between biometric systems and environmental conditions (e.g. illumination, pose variations etc.) and their impact on biometric performance.
- Illustrate of data privacy principles and the impact on the design and configuration of biometric systems.
Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.

| Module 2 |
|---------------------------|-------------------|

| Module 3 |
|---------------------------|-------------------|
| Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment | 8 Hours |

| Module 4 |
|---------------------------|-------------------|
| Multi biometrics: Multi biometrics and multifactor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan | 8 Hours |

| Module 5 |
|---------------------------|-------------------|
| Case studies on Physiological, Behavioral and multifactor biometrics in identification systems | 8 Hours |

**Course Outcomes**

The students should be able to:

- Visualize traditional and biometric systems.
- Analyze different algorithms of biometric systems.
- Compare strengths and weaknesses of different biometric systems.
- Design different biometric system.
- Design multimodal biometric systems.

**Question paper pattern:**
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books**


**Reference Books:**

### Course objectives:
This course will enable students to

- Explain fundamental principles of E-Commerce
- Illustrate technologies & tools for E-Commerce with emphasis on Security
- Identify best techniques & practices for different types of legacy & partner requirements
- Handle & address risk management

### Module 1

### Module 2

### Module 3
Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust. Conceptual model of inter-organizational trust in E-Commerce participation. 8 Hours

### Module 4
Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform. 8 Hours

### Module 5
Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain. 8 Hours

### Course Outcomes
The students should be able to:

- Explain the types of E-Commerce, E-Commerce business models and E-commerce payment systems.
- Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.
- Analysis and explain the issues, risks and challenges in inter-organisational trust in E-Commerce
- Explain the Key components and Trust mechanisms of trusted computing platform.
- Describe the Trusted platforms for organizations and individuals

### Question paper pattern:
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.
<table>
<thead>
<tr>
<th>Text Books</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Books:</td>
</tr>
</tbody>
</table>
INFORMATION SECURITY POLICIES IN INDUSTRY  
[As per Choice Based Credit System (CBCS) scheme] 
(Effective from the academic year 2016 -2017)  
SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>14SFC253</th>
<th>IA Marks</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>03</td>
<td>Exam Marks</td>
<td>80</td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>40</td>
<td>Exam Hours</td>
<td>3</td>
</tr>
</tbody>
</table>

CREDITS – 03

Course objectives: This course will enable students to

- Explain management’s responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Illustrate the differences between the organization’s general information security policy and the needs and objectives of the various issue-specific and system-specific policies the organization will create.
- Know what an information security blueprint is and what its major components are.
- How an organization institutionalizes its policies, standards, and practices using education, training and awareness programs.
- Become familiar with what viable information security architecture is, what it includes, and how it is used.

Module 1

Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

Module 2


Module 3


Module 4

<table>
<thead>
<tr>
<th>Module 1</th>
<th>Teaching Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Information Security Policies</td>
<td>8 Hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 2</th>
<th>Teaching Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Definitions, Standards, Guidelines</td>
<td>8 Hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 3</th>
<th>Teaching Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writing The Security Policies</td>
<td>8 Hours</td>
</tr>
</tbody>
</table>

Module 5

Course Outcomes
The students should be able to:
- Explain the content, need, and responsibilities of information security policies.
- Explain the standards, guidelines, Procedures, and key roles of the organization.
- Able to write policy document for securing network connection and interfaces.
- Explain the threats to the stored data or data in transit and able to write policy document.
- Able to write, monitor, and review policy document.

Question paper pattern:
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

Reference Books:
Course objectives: This course will enable students to

- Fundamental security concepts and architectures that serve as building blocks to database security
- Concepts of user account management and administration, including security risks
- To use current database management system to design and configure the user and data permissions
- Operational components necessary to maximize database security using various security models

Module 1


Module 2


Module 3


Module 4


Module 5


Course Outcomes

The students should be able to:

- Carry out a risk analysis for a large database
• Implement identification and authentication procedures, fine-grained access control and data encryption techniques
• Set up accounts with privileges and roles
• Audit accounts and the database system

**Question paper pattern:**
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books**

**Reference Books:**
1. Database security by Alfred Basta, Melissa Zgola, CENGAGE learning.

---

**MINIPROJECT**

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

**SEMESTER – II**

<table>
<thead>
<tr>
<th>Laboratory Code</th>
<th>16LNI26/ 16SCE26 / 16SCN26 /16SCS26 /16SFC26 / 16SIT26 / 16SSE26</th>
<th>IA Marks</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>03 hours of lab</td>
<td>Exam Marks</td>
<td>80</td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>------</td>
<td>Exam Hours</td>
<td>03</td>
</tr>
</tbody>
</table>

**CREDITS – 02**

**Course objectives:** This course will enable students to
- Enable the student to design, develop and analyze an application development

The student will carry out a mini project relevant to the course. The project must be development of an application (Hardware/Software). It is preferable if the project is based on mobile application development.

**Course outcomes:**
- Design, develop and to analyze an application development.
- Prepare report of the project.

**Conduction of Practical Examination:**
The student shall prepare the report by including:
1. Define project (Problem Definition)
2. Prepare requirements document
   a. Statement of work
   b. Functional requirements
   c. Software / Hardware requirements
3. Develop use cases
4. Research, analyze and evaluate existing learning materials on the application
5. Develop user interface and implement code
6. Prepare for final demo
Evaluation:

Evaluation shall be taken up at the end of the semester. Project work evaluation and viva-voce examination shall be conducted. Internal evaluation shall be carried by the Guide and Head of the department for 20 marks. Final examination which includes demonstration of the project and viva-voce shall be conducted for 80 Marks viz report + Outputs of the project + presentation = 30+30+20 = 80 marks.

SEMINAR

[As per Choice Based Credit System (CBCS) scheme]

(Effective from the academic year 2016-2017)

SEMESTER – II

Subject Code | 16SCE27 / 16SCN27 / 16LNI27 / 16SIT27 / 16SSE27 / 16SCS27 / 16SFC27 | LA Marks | 100
---|---|---|---
Number of Lecture Hours/Week | ---- | Exam Marks | -
Total Number of Lecture Hours | ---- | Exam Hours | -

CREDITS – 01

Course objectives: This course will enable students to

- Motivate the students to read technical article
- Discover recent technology developments

Descriptions

The students should read a recent technical article (try to narrow down the topic as much as possible) from any of the leading reputed and refereed journals like:

1. IEEE Transactions, journals, magazines, etc.
2. ACM Transactions, journals, magazines, SIG series, etc.
3. Springer
4. Elsevier publications etc

In the area of (to name few and not limited to)

- Web Technology
- Cloud Computing
- Artificial Intelligent
- Networking
- Security
- Data mining

Course Outcomes

The students should be able to:

- Conduct survey on recent technologies
- Infer and interpret the information from the survey conducted
- Motivated towards research

Conduction:

The students have to present at least ONE technical seminar on the selected topic and submit a report for internal evaluation.


FILE SYSTEM FORENSIC ANALYSIS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

SEMESTER – IV

Subject Code | IA Marks | Number of Lecture Hours/Week | Exam Marks | Total Number of Lecture Hours | Exam Hours | CREDITS – 04
--- | --- | --- | --- | --- | --- | ---
16SFC41 | 20 | 04 | 80 | 50 | 3

Course objectives: This course will enable students to
- Computer file system and storage analysis
- Basics of Computer forensics
- Role of forensics in business world

Module 1

Module 2

Module 3

Module 4

Module 5
UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries

Course Outcomes
The students should be able to:
- Compare the different file systems for storing information
- Illustrate the role of computer forensics in the business and private world
- Identify some of the current techniques and tools for forensic examinations

Question paper pattern:
The question paper will have ten questions. There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books**

**Reference Books:**

**Laboratory Experiments**
1. Design a simple experiment to test whether a bootable CD/DVD examination altered the hard disk of the suspect’s computer system when the system was booted using the bootable CD/DVD.
2. Design a simple experiments that shows that the correct application of a virtual environment approach results in a less time spent on analysing the evidence, giving more chance of discovering important data, and allowing less qualified personnel to be involved in a more productive way.
3. Write a program to find a unique pattern in each sector of disk.
4. Write a program to compare two partitions.
5. Write a program to compare two disks.
6. Write a program to change or corrupt one byte in a file.

The above experiments can be simulated using freely available forensic tool.

---

**SECURITY ARCHITECTURE DESIGN**

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

**SEMESTER – IV**

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>16SFC421</th>
<th>IA Marks</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>03</td>
<td>Exam Marks</td>
<td>80</td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>40</td>
<td>Exam Hours</td>
<td>3</td>
</tr>
</tbody>
</table>

**CREDITS – 03**

**Course objectives:** This course will enable students to

- Describe the intent of effective site security
- List different security zones
- Select appropriate elements to apply to specific security zones

**Module 1**


**Module 2**

Low-Level Architecture: Code Review, importance of code review, Buffer Overflow | **Teaching Hours** | 8 Hours |

<table>
<thead>
<tr>
<th>Module 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8 Hours</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8 Hours</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8 Hours</strong></td>
</tr>
</tbody>
</table>

**Course Outcomes**

The students should be able to:
- Design the secured sites based on tools & techniques
- Map site zones with level of security
- Identify the components targeted for each zone

**Question paper pattern:**
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books**

**Reference Books:**
# STEGANOGRAPHY AND DIGITAL WATERMARKING

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

SEMESTER – IV

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Number of Lecture Hours/Week</th>
<th>Exam Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SFC422</td>
<td>20</td>
<td>03</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total Number of Lecture Hours</th>
<th>Exam Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>3</td>
</tr>
</tbody>
</table>

CREDITS – 03

**Course objectives:** This course will enable students to

- Basics of Data hiding by using Steganography & Watermarking
- Compare and contrast several different methods of steganography
- Apply digital watermarking as an authentication tool for distribution of content over the Internet

## Module 1

<table>
<thead>
<tr>
<th>Teaching Hours</th>
</tr>
</thead>
</table>


## Module 2

<table>
<thead>
<tr>
<th>Teaching Hours</th>
</tr>
</thead>
</table>

Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

## Module 3

<table>
<thead>
<tr>
<th>Teaching Hours</th>
</tr>
</thead>
</table>

Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.

## Module 4

<table>
<thead>
<tr>
<th>Teaching Hours</th>
</tr>
</thead>
</table>

Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace, binary image, audio, video, Formatting the watermark beds: Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions.

## Module 5

<table>
<thead>
<tr>
<th>Teaching Hours</th>
</tr>
</thead>
</table>

Data Right Management: DRM Products and Laws, Fingerprints, Examples, Protocols and Codes, Boneh-Shaw finger printing Scheme, Steganography and watermarking applications, Military, Digital copyright protection and protection of intellectual property.
Course Outcomes
The students should be able to:

- Distinguish Steganography & Digital watermarking from other related fields.
- Knowledge of how to use steganography techniques in conjunction with encryption systems to protect data.
- Explain different types of watermarking applications and watermarking frameworks.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

Reference Books:

MOBILE DEVICE FORENSICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – IV

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>16SFC423</th>
<th>IA Marks</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lecture Hours/Week</td>
<td>03</td>
<td>Exam Marks</td>
<td>80</td>
</tr>
<tr>
<td>Total Number of Lecture Hours</td>
<td>40</td>
<td>Exam Hours</td>
<td>3</td>
</tr>
<tr>
<td>CREDITS – 03</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Course objectives: This course will enable students to

- Basic Concepts in Mobile Forensics
- Mobile Device Data Storage
- Identify, preserve, extract, analyze, and report data from mobile devices
- Acquiring Evidence from Mobile devices

Module 1

Teaching
<table>
<thead>
<tr>
<th>Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics 8 Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 2 8 Hours</td>
</tr>
<tr>
<td>Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices</td>
</tr>
<tr>
<td>Module 3 8 Hours</td>
</tr>
<tr>
<td>Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.</td>
</tr>
<tr>
<td>Module 4 8 Hours</td>
</tr>
<tr>
<td>Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques</td>
</tr>
<tr>
<td>Module 5 8 Hours</td>
</tr>
<tr>
<td>Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies, Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis</td>
</tr>
</tbody>
</table>

**Course Outcomes**

The students should be able to:

- Describe security risks and vulnerabilities from mobile devices and network access.
- Explain the methods and procedures used in forensics investigations.
- Have knowledge of the global security threats and vulnerabilities of mobile devices and networks.
- Carry out a forensics investigation of mobile and network devices.

**Question paper pattern:**

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books**


**Reference Books:**

SECURITY ASSESSMENT AND VERIFICATION
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>IA Marks</th>
<th>Number of Lecture Hours/Week</th>
<th>Exam Marks</th>
<th>Total Number of Lecture Hours</th>
<th>Exam Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>16SFC424</td>
<td>20</td>
<td>03</td>
<td>80</td>
<td>40</td>
<td>3</td>
</tr>
</tbody>
</table>

**CREDITS – 03**

**Course objectives:** This course will enable students to

- Explain the role of assessment & verification for information security
- Demonstration of different existing tools and procedures for assessment planning
- Recall awareness of risk management

**Module 1**
Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

**Module 2**

**Module 3**
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

**Module 4**

**Module 5**
Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.

**Course Outcomes**
The students should be able to:

- Illustrate the roles information security and its management
- Select appropriate techniques to tackle and solve problems in the discipline of information security assessment
- Design an information security and validation system

**Question paper pattern:**
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.
<table>
<thead>
<tr>
<th>Text Books</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Reference Books:</th>
<th></th>
</tr>
</thead>
</table>