5 Years Integrated M.C.A.

SEC1 Fundamentals of Cyber Security

(060060606)

6th Semester

EFFECTIVE FROM JANUARY - 2018
Course Code: 060060606
Course Title: SEC1 Fundamentals of Cyber Security
Course Credits: 02
[ Lectures: 02, Tutorial: 00, Practical: 00 ]
Prerequisites: Fundamentals of Computers, Internet and Network
Objectives: To imbibe the fundamentals of cybersecurity and its legal perspectives as well as examine the need of cryptography and digital forensics for securing information in the cyber world.

1 Cyber Security [14%]
   1.1. Basic Terminologies: Cybercrime, Cybersecurity, Cyberspace, Cybersquatting, Cyberpunk, Cyberwarfare, and Cyberterrorism
   1.2. Needs of Cyber Security
   1.3. Cyber Criminals: Introduction and Types
   1.4. Planning Cyber Attacks: Phases and Types
   1.5. Cybercrimes Classifications

2 Cyber Offences [16%]
   2.1. Social Engineering: Overview and Classifications
   2.2. Cyberstalking: Types and Working
   2.3. Botnet: Introduction
   2.4. Attack Vector: Overview and Working
   2.5. Mobile Devices Attacks

3 Cybercrime Methods and Security Mechanisms [20%]
   3.1. Phishing: Introduction, Techniques and Prevention
   3.2. Identity Theft: Types, Techniques and Prevention
   3.3. DoS Attack: Classification, Types and Prevention
   3.4. DDoS Attack: Introduction and Prevention
   3.5. SQL Injection: Introduction and Prevention

4 Cryptography and Digital Signature [20%]
   4.1. CIA: Confidentiality, Integrity and Availability
   4.3. Overview of Asymmetric-Key Cryptography
   4.4. Hash Functions: Overview and Usage
   4.6. Digital Signature: Introduction and Importance

5 Legal Perspectives of Cyber Security [12%]
   5.1. Need of Cyber Laws: Reasons for Enactment of Cyber Laws in India
   5.2. Indian ITA: ITA Sections
   5.3. Digital Signature and ITA: Public Key Certificate
   5.4. Representation of Digital Signatures in ITA
   5.5. Cryptographic Perspective of ITA

6 Cyber Forensics Fundamentals [18%]
   6.1. Needs
   6.2. Computer Forensics and Digital Forensics
   6.3. Role of Digital Forensics
   6.4. Rules of Evidence
   6.5. Digital Forensics Phases
   6.6. Digital Forensics Techniques

The tool/platform/technology as an exposure to the concepts’ implementation/demonstration, shall be determined by the course teacher(s) with due approval of Director and/or IQAC.
Course Outcomes: Upon completion of the course, students shall be able to

CO1: Describe cyber crime and its importance including the act of cyber criminals along with its types.
CO2: Classify various types of cyber attacks.
CO3: Classify and relate methods used in cybercrime along with security mechanism.
CO4: Describe basics of cryptography, digital signature and public-key infrastructure in context of cyber security.
CO5: Identify the need for cyber laws, especially in the Indian context.
CO6: Describe the fundamentals of digital forensics with its phases, rules and techniques.

Course Objective and Course Outcomes Mapping:

➢ To imbibe the fundamentals of cybersecurity and its legal perspectives: CO1, CO2, CO3, CO5
➢ Examine the need of cryptography and digital forensics for securing information in the cyber world: CO4, CO5, CO6

Course Units and Course Outcomes Mapping:

<table>
<thead>
<tr>
<th>Unit No.</th>
<th>Unit</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CO1</td>
</tr>
<tr>
<td>1</td>
<td>Cyber Security</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Cyber Offences</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Cybercrime Methods and Security Mechanisms</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>Cryptography and Digital Signature</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Legal Perspectives of Cyber Security</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>Digital Forensics Fundamentals</td>
<td>✓</td>
</tr>
</tbody>
</table>

Hands-on Activity

➢ Hands-on sessions shall be conducted on following topics:
   1. Steganography
   2. Symmetric-Key Cryptography

Modes of Transaction(Delivery):

➢ Lecture method shall be used for all units. For all units lecture delivery shall be supplemented with audio-visual aids.
➢ Self-Study of following part of the syllabus shall be done by the students: 2.5: Mobile Devices Attacks

Activities/Practicum:

The following activities shall be carried out by the students.
➢ Discuss real case studies of cyber stalking and phishing.
➢ Implementation of at least one algorithm of Symmetric-Key Cryptography/Asymmetric-Key Cryptography in any technology.
The following activities shall be carried out by the teacher.
- Show demonstration of NMAP/SQLmap tool.
- Show demonstration of security settings in personal computer.

Text Books:

Reference Books:
2. George M. Mohay - Computer and Intrusion Forensics - Artech House

Concept Map:
It is a hierarchical / tree based representation of all topics covered under the course. This gives direct / indirect relationship / association among topics as well as subtopics.

Unit 1: Cyber Security

Unit 2: Cyber Offenses
Unit 3: Cyber Crime Methods and Security Mechanisms

Unit 4: Cryptography and Digital Signature
Unit 5: Legal Perspectives of Cyber Security

Legal Perspectives of Cyber Security

- Need of Cyber Laws
- Reasons for Enactment of Cyber Laws in India
- Indian ITA
- ITA Sections
- Cryptographic Perspective of ITA
- Representation of Digital Signatures in ITA
- Digital Signature and ITA: Public Key Certificate

Unit 6: Cyber Forensics Fundamentals
Assessment:

- The weightage of Continuous Internal Evaluation (CIE) and University examination shall be as per the University regulations.
- The course teacher is free to decide the structure of CIE:
  - i. Assessment parameters like Open Book test, Quizzes, Unit Tests, Assignments, Internal, Self-Creation and/or assessment parameters of student's activity defined under Activities/Practicum.
  - ii. Weightage and frequency of each parameter.
- After assessment parameters are approved by Director and/or IQAC, the parameter list shall be informed to the students by publishing over web before commencement of the semester.
- The assessment policy document should be uploaded on the web before the commencement of the semester.
- Syllabus for each CIE parameter shall be covered by the date of the corresponding test.
- No make-up work shall be conducted unless approval from Programme Co-ordinator/Director.

UFM:

- Any ascertained fact of breaking institute policy shall be associated with one or all of the following: (i) zero marks for the work; (ii) report to the programme coordinator; (iii) report to the Director.

Attendance:

- Attendance means being present for the entire class session. Those arriving significant late or leaving significantly early without prior permission shall be counted as ABSENT for the entire class session.
- Concern teacher must clearly state his/her attendance policies at the first class meeting.