|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cryptography and Network Security**  **(Effective from the Academic Year 2023 – 2024)**  **VI SEMESTER** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Course Code | | | | | | | | | **21IS653** | | | | | | CIA Marks | | | | | | | | | | 50 | |
| Number of Contact Hours/Week (L: T: P: S) | | | | | | | | | 3:0:0:0 | | | | | | SEE Marks | | | | | | | | | | 50 | |
| Total Hours of Pedagogy | | | | | | | | | **40L** | | | | | | Exam Hours | | | | | | | | | | 03 | |
| **CREDITS – 3** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **COURSE PREREQUISITES:**   * Fundamental knowledge of Cryptography Theories and Network security. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **COURSE OBJECTIVES:**   * This course is aimed at providing students with a practical and theoretical knowledge of cryptography and network security. * To develop an understanding of different cryptographic protocols and techniques. * To understand methods for authentication, access control, intrusion detection and prevention. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **TEACHING - LEARNING STRATEGY:**  Following are some sample strategies that can be incorporate for the Course Delivery   * Chalk and Talk Method/Blended Mode Method * Power Point Presentation * Expert Talk/Webinar/Seminar * Video Streaming/Self-Study/Simulations * Peer-to-Peer Activities * Activity/Problem Based Learning * Case Studies * MOOC/NPTEL Courses * Any other innovative initiatives with respect to the Course contents | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **COURSE CONTENTS** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **MODULE - I** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Introduction to Network Security:** Introduction - Need for Security, Security Approaches, Principles of Security, Security services, Types of Attacks – General View - Technical View, Programs that Attack, Specific Attacks. | | | | | | | | | | | | | | | | | | | | | | | | | **8 Hours** | |
| **MODULE - II** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Basics of Cryptography and Encryption:** Introduction to Cryptography, Plain Text and Cipher Text, Symmetric Cipher Model, Cryptography, Cryptanalysis, Brute Force Attacks, Substitution Techniques - Caesar Cipher and Modified Caesar Cipher, Mono Alphabetic cipher, Poly-Alphabetic Cipher, Playfair Cipher, Transposition Techniques- Rail Fence technique, Simple Columnar transposition Technique. | | | | | | | | | | | | | | | | | | | | | | | | | **8 Hours** | |
| **MODULE - III** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Block ciphers and Data encryption standards:** Stream ciphers Block ciphers, Data Encryption Standard, a DES example, AES- structure, AES transformation functions. | | | | | | | | | | | | | | | | | | | | | | | | | **8 Hours** | |
| **MODULE - IV** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Public key cryptography and RSA:** Principles of public key cryptosystems - public key cryptosystems - applications for public key cryptosystems, RSA algorithm - algorithm and example.  **Cryptographic Data integrity algorithms** - Cryptographic Hash functions - applications, Message Authentication – Requirements and Functions. | | | | | | | | | | | | | | | | | | | | | | | | | **8 Hours** | |
| **MODULE - V** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Applications of network and internet security:** Cloud computing- Data protection on the cloud, cloud security as a service, Web/Internet security protocols- HTTPS, SSL, SSH, Wireless network security, Mobile device security, Email Security-Pretty good privacy, S/MIME.  **Legal and Ethical issues-** Introduction to Cybercrime & computer crime, Intellectual property, Privacy, Ethical issues. | | | | | | | | | | | | | | | | | | | | | | | | | **8 Hours** | |
| **COURSE OUTCOMES** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Upon completion of this course, the students will be able to: | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **CO**  **No.** | **Course Outcome Description** | | | | | | | | | | | | | | | | | | | | | | | **Bloom’s Taxonomy Level** | | |
| CO1 | Understand the fundamentals of networks security, security architecture, threats and vulnerabilities | | | | | | | | | | | | | | | | | | | | | | | CL2 | | |
| CO2 | Apply the different cryptographic operations of symmetric cryptographic algorithms. | | | | | | | | | | | | | | | | | | | | | | | CL3 | | |
| CO3 | Apply the different cryptographic operations of public key cryptography | | | | | | | | | | | | | | | | | | | | | | | CL3 | | |
| CO4 | Apply the various Authentication schemes to simulate different applications. | | | | | | | | | | | | | | | | | | | | | | | CL3 | | |
| CO5 | Understand various Security practices and System security standards. | | | | | | | | | | | | | | | | | | | | | | | CL4 | | |
| **CO-PO-PSO MAPPING** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **CO**  **No.** | **Programme Outcomes (PO)** | | | | | | | | | | | | | | | | | | | | | **Programme Specific Outcome (PSO)** | | | | |
| **1** | **2** | | **3** | **4** | | **5** | **6** | | **7** | | | **8** | **9** | | **10** | | | | **11** | **12** | **1** | | | | **2** |
| **CO1** | 3 | 1 | | 1 | 1 | | 1 |  | |  | | |  | 2 | | 1 | | | | 3 | 2 | 2 | | | | 1 |
| **CO2** | 3 | 3 | | 3 | 2 | | 3 |  | | 1 | | |  | 2 | | 1 | | | | 2 | 2 | 3 | | | | 1 |
| **CO3** | 3 | 3 | | 2 | 2 | | 3 |  | |  | | |  | 1 | | 1 | | | | 2 | 2 | 3 | | | | 2 |
| **CO4** | 2 | 3 | | 3 | 2 | | 3 |  | |  | | |  | 2 | | 1 | | | | 2 | 3 | 2 | | | | 2 |
| **CO5** | 2 | 3 | | 3 | 2 | | 2 | 2 | |  | | |  | 3 | | 1 | | | | 2 | 3 | 3 | | | | 3 |
| **3: Substantial (High)** | | | | | | | **2: Moderate (Medium)** | | | | | | | | | **1: Poor (Low)** | | | | | | | | | | |
| **ASSESSMENT STRATEGY**  Assessment will be both CIA and SEE. Students learning will be assessed using Direct and Indirect methods: | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Sl. No.** | **Assessment Description** | | | | | | | | | | | **Weightage (%)** | | | | | | | **Max. Marks** | | | | | | | |
| **1** | **Continuous Internal Assessment (CIA)** | | | | | | | | | | | **100 %** | | | | | | | **50** | | | | | | | |
|  | Continuous Internal Evaluation (CIE) | | | | | | | | | | | 60 % | | | | | | | 30 | | | | | | | |
| Assignments | | | | | | | | | | | 40 % | | | | | | | 20 | | | | | | | |
| **2** | **Semester End Examination (SEE)** | | | | | | | | | | | **100 %** | | | | | | | **50** | | | | | | | |
| **ASSESSMENT DETAILS** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Continuous Internal Assessment (CIA) (50%)** | | | | | | | | | | | | | | | | | | **Semester End Exam (SEE) (50%)** | | | | | | | | |
| **Continuous Internal Evaluation (CIE) (60%)** | | | | | | | | | | | **Assignment/**  **Activities (40%)** | | | | | | |
| **I** | | | **II** | | | **III** | | | | |
| **Syllabus Coverage** | | | | | | | | | | | **Syllabus Coverage** | | | | | | | **Syllabus Coverage** | | | | | | | | |
| **40%** | | | **30%** | | | **30%** | | | | | **100%** | | | | | | | **100%** | | | | | | | | |
| MI | | |  | | |  | | | | | MI | | | | | | | MI | | | | | | | | |
| MII | | | MII | | |  | | | | | MII | | | | | | | MII | | | | | | | | |
|  | | | MIII | | |  | | | | | MIII | | | | | | | MIII | | | | | | | | |
|  | | |  | | | MIV | | | | | MIV | | | | | | | MIV | | | | | | | | |
|  | | |  | | | MV | | | | | MV | | | | | | | MV | | | | | | | | |
| ***Note: For Examinations (both CIE and SEE), the question papers shall contain the questions mapped to the appropriate Bloom’s Level. Any COs mapped with higher cognitive Bloom’s Level may also be assessed through the assignments.*** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **ASSIGNMENT TYPES WITH WEIGHTAGES** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Sl. No.** | **Assignment Description** | | | | | | | | | | | | | | | | **Max. Weightage (%)** | | | | | | **Max. Marks** | | | |
| 1 | Written Assignments | | | | | | | | | | | | | | | | 25 % | | | | | | 05 | | | |
| 2 | Quiz | | | | | | | | | | | | | | | | 10 % | | | | | | 02 | | | |
| 3 | Case Studies | | | | | | | | | | | | | | | | 25 % | | | | | | 05 | | | |
| 4 | Seminar/Presentation | | | | | | | | | | | | | | | | 15 % | | | | | | 03 | | | |
| 5 | Peer - to - Peer Learning | | | | | | | | | | | | | | | | 10 % | | | | | | 02 | | | |
| 6 | Activity Based Learning | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| 7 | Project Based Learning | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| 8 | Field Work + Report | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| 9 | Industry Visit + Report | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| 10 | NPTEL/MOOC Courses – Registration and Assignment Submissions | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| NPTEL Certification | | | | | | | | | | | | | | | | 75 % | | | | | | 15 | | | |
| 11 | Any other Innovative Assignments (CL4 and above) | | | | | | | | | | | | | | | | 50 % | | | | | | 10 | | | |
| ***Note: The assignments mentioned above may be provided appropriately to the students belonging to different bands*** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **SEE QUESTION PAPER PATTERN:**   * The question paper will have **TEN** full questions from **FIVE** Modules * There will be 2 full questions from each module. Every question will carry a maximum of 20 marks. * Each full question may have a maximum of four sub-questions covering all the topics under a module. * The students will have to answer FIVE full questions, selecting one full question from each module. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **TEXT BOOKS:**   1. AtulKahate, Cryptography and Network Security, 4th Edition,2019 2. William Stallings, Cryptography and Network Security: Principles and Practices, 7th Edition,2019. 3. Nina Godbole and SunitBelapure, Cyber Security, 1st Edition, 2019. | | | | | | | | | | | | | | | | | | | | | | | | | | |

|  |
| --- |
| **REFERENCE WEB LINKS AND VIDEO LECTURES (E - RESOURCES):**   1. <https://www.geeksforgeeks.org/cryptography-and-network-security-principles> 2. https://www.codingninjas.com/studio/library/cryptography-and-network-security |