**Detailed Syllabus**

.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Course Code** | 15B17CI576 | **Semester** Odd  **(specify Odd/Even)** | | **Semester 5th Session** 2023 -2024  **Months from** July 2023 **to** December 2023 | |
| **Course Name** | Information Security Lab | | | | |
| **Credits** | 1 | | **Contact Hours** | | 2 |

|  |  |  |
| --- | --- | --- |
| **Faculty (Names)** | **Coordinator(s)** | J62:Mradula Sharma J128: Dr. Shariq |
| **Teacher(s) (Alphabetically)** | J-62: Dr. Amanpreet Kaur,Mradula Sharma, Dr. SharddhaPorwal, Dr. Somya Jain, Dr. Raghu Vamsi |

|  |  |  |
| --- | --- | --- |
| **Course Outcomes (CO)** | **Description** | **Cognitive Level (Bloom’s Taxonomy)** |
| **C374.1** | Demonstrate and illustrate the different cipher techniques and understand various anti-virus and anti worms | Level-2  (Understanding Level) |
| **C374.2** | Develop and make a code to implement various Symmetric key , Asymmetric key cryptographic techniques and steganography techniques | Level-3  (Applying Level) |
| **C374.3** | Apply a client server programming for symmetric ,asymmetric algorithms and key exchange algorithms, Application of information security to real world problems | Level-3  (Applying Level) |
| **C374.4** | Examine and analyze the packet information for different protocols using Wireshark. | Level-4  (Analyzing Level) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Module No.** | **Title of the Module** | **List of Experiments** | **CO** |
| 1. | Cryptography | Introduction to Cryptography | C374.1 |
| 2. | Ciphers | Implementation of Cipher using Transposition techniques and Caesar Cipher | C374.2 |
| 3. | Ciphers | Implementation of Substitution Ciphers: Hill Cipher and Polyalphabetic Cipher | C374.2 |
| 4. | Symmetric key cryptography | Introduction to Symmetric key cryptography | C374.1 |
| 5. | Data Encryption Standard | Implementation of Data Encryption Standard ( DES) | C374.2 |
| 6. | Public key cryptography | Introduction to Public key cryptography and Digital signature | C374.2 |
| 7. | Key Exchange Algorithm | Implementation of Diffie Hellman Key Exchange Algorithm | C374.3 |
| 8. | Client server programming | Client server programming using TCP | C374.3 |
| 9. | Client server programming | Implementation of DES and RSA using Client server programming | C374.3 |
| 10. | Steganography | Introduction to Steganography | C374.2 |
| 11. | Antivirus and Anti-Worms | Introduction to Antivirus and Anti-Worms, and Wireshark tool | C374.1 |
| 12. | Applications of Information Security | Applications of Information Security to real world problems | C374.3 |
| 13. | Wireshark | Understanding of Secure-socket layer, Application Layer (HTTP, FTP, DNS) using Wireshark tool | C374.4 |
| **Evaluation Criteria**  **Components Maximum Marks**  Lab Test -1 20  Lab Test -2 20  Eval 1 15  Eval2 15  Project 15  Attendance 15  **Total 100** | | | |
|  | | | |

Project based learning: The students are grouped into groups of size 5-6 and will be implementing a secure client server program with required encryption techniques. The student will analyze the requirements and select the required solutions. This will help in the employability of students in the information security sector.

|  |  |
| --- | --- |
| **Recommended Reading material:** Author(s), Title, Edition, Publisher, Year of Publication etc. (Text books, Reference Books, Journals, Reports, Websites etc. in the IEEE format) | |
| 1. | Information Security, Principles and Practice, , 2nd Edition, Mark Stamp, Wiley, 2011 |
| 2. | Security in Computing 5thEdition , Charles P Fleeger et. al. - Prentice Hall, 2015 |
| 3. | The InfoSec Handbook: An Introduction to Information Security- Apress Open, Nayak, Umesha, and UmeshHodeghatta Rao, 2014 |
| 4. | Information Security: The Complete Reference, 2ndEdition- Mark Rhodes Ousley, 2013 |
| 5. | Cracking Codes with Python: An Introduction to Building and Breaking Ciphers-Al Sweigart, 2018 |