**COEP Technological University, Pune**

**Teaching Plan- Theory (July 2025-December 2025)**For display

**Name of the Faculty: Vinod Pachghare Course: Cryptography and Network Security Course Code:**

**Exam Scheme: TA:20-MSE:30—ESE:50 Class: B. Tech CSE DIV-II Teaching Scheme: 3 Hrs/week**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sr No | Date | Day | Lecture No. | Timing | Unit No. | Topic to be covered | Ref.  Book / PPT/ Link | \*Teaching methodology / Instructional Strategy |
|  | 21-7-25 | Monday | 1 | 3:30 to 4:30 | 1 | Introduction: Cryptography and modern cryptography, Need of security | V. K. Pachghare, “Cryptography and Information Security”, 3rd edition, PHI Learning, ISBN: 978-93-893-4710-4  William Stallings, “Cryptography and Network Security, Principles and Practices”, Pearson Education, Fifth Edition, ISBN: 0-13-60970-9 | Chalk & Board, PPT |
|  | 22-7-25 | Tuesday | 2 | 3:30 to 4:30 | 1 | Security services, Basic network security terminology | Chalk & Board, PPT |
|  | 23-7-25 | Wednesday | 3 | 3:30 to 4:30 | 1 | Security attacks | Chalk & Board, PPT |
|  | 28-7-25 | Monday | 4 | 2:30 to 3:30 | 1 | Classical cryptosystems and their cryptanalysis | Chalk & Board, PPT |
|  | 29-7-25 | Tuesday | 5 | 2:30 to 3:30 | 1 | Operational model of network security | Chalk & Board, PPT |
|  | 30-7-25 | Wednesday | 6 | 2:30 to 3:30 | 1 | One Time Pad | Chalk & Board, PPT |
|  | 4-8-25 | Monday | 7 | 2:30 to 3:30 | 2 | Prime Number, relatively prime numbers, Modular Arithmetic | Chalk & Board, PPT/ Flipped Class |
|  | 5-8-25 | Tuesday | 8 | 2:30 to 3:30 | 2 | Fermat’s and Euler’s Theorem | Chalk & Board, PPT/ Flipped Class |
|  | 6-8-25 | Wednesday | 9 | 2:30 to 3:30 | 2 | The Euclidean and Extended Euclidean Algorithms | Chalk & Board, PPT/ Flipped Class |
|  | 11-8-25 | Monday | 10 | 2:30 to 3:30 | 2 | Totient Function | Chalk & Board, PPT/ Flipped Class |
|  | 12-8-25 | Tuesday | 11 | 2:30 to 3:30 | 2 | The Chinese Remainder Theorem | Chalk & Board, PPT/ Flipped Class |
|  | 13-8-25 | Wednesday | 12 | 2:30 to 3:30 | 2 | Discrete logarithms | Chalk & Board, PPT |
|  | 18-8-25 | Monday | 13 | 2:30 to 3:30 | 3 | Symmetric Key Ciphers, Feistel Networks | Chalk & Board, PPT |
|  | 19-8-25 | Tuesday | 14 | 2:30 to 3:30 | 3 | Modern Block Ciphers: DES | Chalk & Board, PPT |
|  | 20-8-25 | Wednesday | 15 | 2:30 to 3:30 | 3 | Modern Block Ciphers: AES | Chalk & Board, PPT |
|  | 25-8-25 | Monday | 16 | 2:30 to 3:30 | 3 | Modern Block Ciphers: IDEA | Chalk & Board, PPT |
|  | 26-8-25 | Tuesday | 17 | 2:30 to 3:30 | 3 | Modes of Operation | Chalk & Board, PPT |
|  | 1-9-25 | Monday | 18 | 2:30 to 3:30 | 3 | Cryptanalysis of Symmetric Key Ciphers: Linear Cryptanalysis | Chalk & Board, PPT |
|  | 2-9-25 | Tuesday | 19 | 2:30 to 3:30 | 3 | Differential Cryptanalysis | Chalk & Board, PPT |
|  | 3-9-25 | Wednesday | 20 | 2:30 to 3:30 | 4 | **Asymmetric Cryptography**: RSA | Chalk & Board, PPT |
|  | 15-9-25 | Monday | 21 | 2:30 to 3:30 | 4 | Key Distribution and Management | Chalk & Board, PPT |
|  | 16-9-25 | Tuesday | 22 | 2:30 to 3:30 | 4 | Diffie-Hellman Key Exchange | Chalk & Board, PPT |
|  | 17-9-25 | Wednesday | 23 | 2:30 to 3:30 | 4 | Elliptic Curve Cryptography | Chalk & Board, PPT |
|  | 22-9-25 | Monday | 24 | 2:30 to 3:30 | 4 | hash functions: The Merkle Damgard Construction | Chalk & Board, PPT |
|  | 23-9-25 | Tuesday | 25 | 2:30 to 3:30 | 4 | Message Digest algorithms: MD5 | Chalk & Board, PPT |
|  | 24-9-25 | Wednesday | 26 | 2:30 to 3:30 | 4 | Secure Hash algorithm (SHA) | Chalk & Board, PPT |
|  | 29-9-25 | Monday | 27 | 2:30 to 3:30 | 4 | Message Authentication Codes | Chalk & Board, PPT |
|  | 30-9-25 | Tuesday | 28 | 2:30 to 3:30 | 5 | **Authentication and Web Security**: Introduction | Chalk & Board, PPT |
|  | 1-10-25 | Wednesday | 29 | 2:30 to 3:30 | 5 | Digital Signatures | Chalk & Board, PPT |
|  | 6-10-25 | Monday | 30 | 2:30 to 3:30 | 5 | Authentication Protocols, Kerberos, | Chalk & Board, PPT |
|  | 7-10-25 | Tuesday | 31 | 2:30 to 3:30 | 5 | X.509 | Chalk & Board, PPT |
|  | 8-10-25 | Monday | 32 | 2:30 to 3:30 | 5 | Digital Certificate Standard |  | Chalk & Board, PPT |
|  | 13-10-25 | Tuesday | 33 | 2:30 to 3:30 | 5 | Pretty Good Privacy |  | Chalk & Board, PPT/ Flipped Class |
|  | 14-10-25 | Wednesday | 34 | 2:30 to 3:30 | 5 | Secure Socket Layer |  | Chalk & Board, PPT |
|  | 15-10-25 | Monday | 35 | 2:30 to 3:30 | 5 | Secure Electronic Transaction. Zero knowledge proof |  | Chalk & Board, PPT |
|  | 27-10-25 | Monday | 36 | 2:30 to 3:30 | 6 | **Network Security**: Intruders, Intrusion Detection |  | Chalk & Board, PPT/ Flipped Class |
|  | 28-10-25 | Tuesday | 37 | 2:30 to 3:30 | 6 | Password Management, Worms, viruses, Trojans, Virus Countermeasures |  | Chalk & Board, PPT |
|  | 29-10-25 | Wednesday | 38 | 2:30 to 3:30 | 6 | Firewalls, Firewall Design Principles |  | Chalk & Board, PPT |
|  | 3-11-2025 | Monday | 39 | 2:30 to 3:30 | 6 | Vulnerabilities in TCP/IP model |  | Chalk & Board, PPT |
|  | 4-11-25 | Tuesday | 40 | 2:30 to 3:30 | 6 | Vulnerabilities in TCP/IP model |  | Chalk & Board, PPT/ Flipped Class |

**\*Teaching methodology / Instructional Strategy:** can be one or more (Chalk& Board, Lecture, Q & A, Seminar, Group Discussion, Video-showcase, Demonstration, Project Based Learning / Active Learning, Collaborative Learning, Experiential Learning, Field Visit, Self-Learning, Computer Assisted Learning (CAL), MOOC, Problem Solving, Flipped Class, etc.)

**Displayed to students on ( Provide Date): 1 August 2025**

**Provide Remarks regarding content, Innovation in Pedagogy etc):**

**Faculty Member Head of the Department**