## DSM352Data Privacy and Security

| | | |
|---|---|---|
| **Semester: V** | **Course Title:** Data Privacy and Security | Credit: 4 |
| **Course Code:** DSM352 | | (3 T + 1 P) |

**Course Outcomes: On successful completion of the course the learner will be able to**

| CO | COGNITIVEABILITIES | COURSEOUTCOMES |
|---|---|---|
| CO1 | REMEMBERING | Recall fundamental security goals, cryptographic principles, and common ciphers. |
| CO2 | UNDERSTANDING | Explain symmetric/asymmetric encryption algorithms, hashing, and digital signatures. |
| CO3 | APPLYING | Apply cryptographic algorithms, steganographic techniques, and secure communication protocols. |
| CO4 | ANALYSING | Analyze vulnerabilities, attacks, and security risks in digital systems. |
| CO5 | EVALUATING | Evaluate privacy policies, security mechanisms, and legal compliance requirements. |
| CO6 | CREATING | Design secure systems incorporating cryptography, data hiding, and privacy-by-design principles. |

| | PSO 1 | PSO 2 | PSO 3 | PSO 4 | PSO 5 |
|---|---|---|---|---|---|
| CO 1 | 3 | 3 | 2 | 2 | 1 |
| CO 2 | 2 | 3 | 3 | 2 | 1 |
| CO 3 | 2 | 3 | 2 | 3 | 2 |
| CO 4 | 2 | 3 | 3 | 2 | 2 |
| CO 5 | 3 | 3 | 3 | 2 | 1 |
| CO 6 | 3 | 3 | 3 | 3 | 2 |

| Unit No. | Detailed Syllabus | Teaching Hours |
|---|---|---|
| I | **Introduction to Security and Ciphers**<br>Introduction: Security goals, cryptographic attacks, services and mechanisms, techniques.<br>Traditional Symmetric Key Ciphers: Substitution ciphers, transposition ciphers, stream and block ciphers.<br>Modern Symmetric-Key Ciphers: Modern block ciphers, modern stream ciphers. | 15 |
| II | **Core Cryptographic Techniques**<br>Symmetric Encryption: DES (structure, multiple DES, security), AES (transformations, key expansion, cipher structure, basic security analysis).<br>Asymmetric Encryption: RSA basics, key generation, encryption/decryption.<br>Hash Functions: Purpose and properties, SHA-512 overview.<br>Digital Signatures: Concept, process, and applications.<br>Basic Data Hiding: Introduction to steganography, simple LSB technique in images. | 15 |
| III | **Privacy, Legal, and Ethical Issues**Privacy concepts, principles, and policies. Authentication and privacy. Privacy issues in data mining, web browsing, and email security. Impacts of emerging technologies (IoT, AI) on | 15 |

| | | |
|---|---|---|
| | privacy. Legal aspects: data protection laws (GDPR, HIPAA, CCPA), protecting programs and data, information law, rights of employees and employers, redress for software failures, computer crime. Ethical issues in cybersecurity: professional responsibilities, ethical hacking. | |
| **IV** | **Practical Component (Using Python)**<br><br>• Implement substitution and transposition ciphers.<br>• DES/AES encryption/decryption program.<br>• RSA key generation, encryption and decryption.<br>• Creating and verifying digital signature<br>• Implement symmetric and asymmetric encryption and decryption in Python.<br>• Perform hashing and verify integrity using SHA algorithms.<br>• Apply access control simulation using role-based permissions.<br>• Conduct a basic vulnerability scan using open-source tools.<br>• Log analysis and anomaly detection scripts.<br>• Mini projects: secure file transfer, encrypted chat application, data anonymization script. | **15** |

**Suggested Reference Books:**


- Stallings, W. – Cryptography and Network Security: Principles and Practice, Pearson.
- Kaufman, C., Perlman, R., Speciner, M. – Network Security: Private Communication in a Public World, Pearson.
- Pfleeger, C. P., Pfleeger, S. L., Margulies, J. – Security in Computing, Pearson.
- Shostack, A. – Threat Modeling: Designing for Security, Wiley.
- Solove, D. J., Schwartz, P. M. – Information Privacy Law, Aspen Publishers.
- Andress, J. – The Basics of Information Security, Syngress.


H.O.D
Dept of DATA SCIENCE & ANALYTICS
M.G. Science Institute, Ahmedabad-9.