of information and network security.
2) To equip students with the knowledge and skills to implement cryptographic techniques and network security mechanisms.
3) To introduce students to secure software development practices and application security.
4) To explore advanced topics in security, including incident response, forensics, and emerging security challenges.
5) To prepare students to assess, design, and manage secure information systems and networks.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamental concepts of information security, including threat models, security policies, and risk management.
CO2	Implement cryptographic algorithms and protocols to secure communication and data.
CO3	Apply network security techniques, including firewalls, intrusion detection, VPNs, and wireless security.
CO4	Develop secure software applications and mitigate web, mobile, cloud, and database security threats.
CO4	Engage with advanced security topics, conduct incident response and forensics, and address security challenges in emerging technologies.

S. NO	Contents	Contact Hours

UNIT 1	**Introduction to Information Security:** Overview: Definitions, Objectives, and Importance Security Threats and Vulnerabilities: Malware, Phishing, Social Engineering, and Insider Threats. Security Models: CIA Triad (Confidentiality, Integrity, Availability), Bell-LaPadula, and Biba Models Security Policies and Mechanisms: Authentication, Authorization, and Access Control Risk Management: Risk Assessment, Mitigation Strategies, and Security Audits	**10**
UNIT 2	**Cryptography** Introduction to Cryptography: Definitions and Goals Symmetric Key Cryptography: Algorithms (DES, AES), Modes of Operation, and Key Management Asymmetric Key Cryptography: RSA, ECC, and Digital Signatures Hash Functions: SHA, MD5, and Applications of Hashing Cryptographic Protocols: SSL/TLS, PGP, and Key Exchange Protocols	**12**
UNIT 3	**Network Security** Overview of Network Security: Goals, Threats, and Attack Vectors Firewalls: Types, Configuration, and Best Practices Intrusion Detection and Prevention Systems (IDPS): Techniques and Tools Virtual Private Networks (VPNs): Architecture, Protocols (IPSec, SSL VPN), and Applications Wireless Network Security: WEP, WPA, WPA2, and Wireless Attack Vectors	**10**
UNIT 4	**Application and Web Security** Secure Software Development: Secure Coding Practices, OWASP Top 10, and Threat Modeling Web Security: Cross-Site Scripting (XSS), SQL Injection, CSRF, and Secure Session Management Security in Mobile Applications: Common Threats, Security Frameworks, and Best Practices Cloud Security: Threats in Cloud Computing, Security Models, and Cloud Security Standards Database Security: SQL Injection Prevention, Data Encryption, and Access Control	**10**
UNIT 5	**Advanced Topics in Information and Network Security** Cybersecurity Frameworks and Standards: ISO 27001, NIST, and GDPR Compliance Incident Response and Forensics: Phases of Incident Response, Digital Forensics Tools, and Techniques Security in Emerging Technologies: IoT Security, Blockchain Security, and AI in Security Ethical Hacking and Penetration Testing: Methodologies, Tools, and Legal Aspects Future Trends in Information and Network Security: Quantum Cryptography, Zero Trust Security, and 5G Security	**10**

	TOTAL	**42**