

B.Tech.IV Year ISem.

CS4101PC: INFORMATION SECURITY

IV-I:CSE								
Course Code	Category	Hours/Week			Credits	Max Marks		
CS4101PC	Core	L	T	P	C	CIE	SEE	Total
		3	0	0	3	25	75	100
Contact Classes:45	Tutorial classes:15	Practical classes: Nill				Total Classes:60		
Prerequisites								

Course Objectives:

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.
- Discuss Web security and Firewalls

Course Outcomes:

- Student will be able to understand basic cryptographic algorithms, message and web authentication and security issues.
- Ability to identify information system requirements for both of them such as client and server.
- Ability to understand the current legal issues towards information security.

UNIT-I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network

Security Cryptography Concepts and Techniques: Introduction, plaintext and ciphertext, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

UNIT-II

Symmetric Key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

Asymmetric Key Ciphers: Principles of public key cryptosystems, RSA algorithm, ElGamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

UNIT-III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), **Message authentication codes:** Authentication requirements, HMAC, CMAC, Digital signatures, ElGamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric &

Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public-Key Infrastructure

UNIT-IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH)

Wireless Network Security:

Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security

UNIT-V

E-

Mail Security: Pretty Good Privacy, S/MIME **IP Security:** IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange

Case Studies on Cryptography and security : Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Crosssite Scripting Vulnerability.

TEXTBOOKS:

1. Cryptography and Network Security-Principles and Practice:
William Stallings, Pearson Education, 6th Edition
2. Cryptography and Network Security: Atul Kahate, McGraw Hill, 3rd Edition

REFERENCE BOOKS:

1. Cryptography and Network Security: CK Shyamala, N Harini, Dr TR Padmanabhan,
Wiley India, 1st Edition.
2. Cryptography and Network
Security: Forouzan Mukhopadhyay, McGraw Hill, 3rd Edition
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning
6. Network Security and Cryptography : Bernard Menezes, CENGAGE Learning