Branch: B.Sc.(IT)	Semester-V
Subject Code: 5103	Lecture: 04 Credit: 04
Course Opted	Core Course - 17
Subject Title	INTERNET SECURITY

Course Objectives:

- Introducing the arena of Internet security & related concepts to the students.
- To understand various concepts related to data confidentiality.
- To expertise the art of Cryptography & various related techniques.
- To learn implementation of digital signature & digital signature certificate.
- To learn various authentication mechanism.
- To learn about various internet security protocols.
- Learning about firewall, its various configurations & implementation.
- Real world case studies.

Course Outcomes:

- Complete understanding of various threats faced by the Internet and related services.
- Protection against cyber-attacks by implementing various security protocols.
- Understanding nature of various cyber-attacks & developing defences against such attacks.

Modules	Sr. No.	Topic and Details	No of Lectures Assigned	Marks Weightage %
UNIT - I	1	Introduction: Need for security, security approaches, principles of security, Types of attacks, types of attacks on cipher text, cryptanalyst	5	10
	2	Cryptographic techniques: Plain text and Cipher text, Substitution Techniques, Transposition Techniques, Encryption, decryption, Symmetric, Asymmetric Key Cryptography, Data Encryption Standard (DES), IDEA,RC5, Blowfish, AES	5	10
	3	Asymmetric Key Cryptography, The RSA algorithm, Symmetric and Asymmetric Key Cryptography together, Digital signatures and related algorithms, Modular Arithmetic (addition, multiplication, inverse, exponentiation)	5	10
UNIT-II	4	Public Key Infrastructure (PKI): Digital Signatures, Digital Certificates, Private key management, the PKIX model, PKCS, XML, PKI and security	5	10
	5	Internet Security Protocols: Basic concepts, SSL, SHTTP,TSP, SET, SSL versus SET,3D secure protocol, Electronic Money, Email security, WAP security	5	10
	6	Authentication: Password Based, Address Based, Cryptographic Authentication, Passwords,	5	10

		Cryptographic Authentication: passwords as keys, protocols, KDC's, Certification Authorities, Authentication of People: Verification techniques, passwords, length of passwords, password distribution, smart cards, biometric authentication		
UNIT-III	7	Network Security: Brief introduction to Network Security, Firewalls, IP security, Virtual Private Network (VPN), system security: Intruders and Viruses, Firewalls, Intrusion Detection	5	10
	8	Case Studies on Cryptography and security: Cryptographic Solutions, SSO, Secure inter-branch Payment Transactions, Denial Of Service (DOS) attacks, IP Spoofing attacks, CSSV, Secrete splitting, Contract signing	5	10
UNIT-IV	9	Study of real attacks on computer systems and networks of the following kind: Hacking attack, Denial Of Service (DOS) attacks, IP Spoofing attacks, CSSV	5	10
	10	Example System: Kerberos: purpose, authentication, Security in GSM, server and ticket granting, server, keys and tickets, use of AS and TGS, replicated servers, Kerberos V4: names, inter-realm , authentication, key version numbers , Kerberos V5: names, realms, delegation, forwarding and proxies, ticket lifetimes, revoking tickets, multiple Realms	5	10
		TOTAL	**50**	**100**

Text Book:

1. Atul Kahate, Cryptography and Network Security, McGraw Hill

Reference Books:

1. Kaufman, C., Perlman, R.,& Speciner, M., .Network Security, Private Communication in a Public world, 2nd ed., Prentice Hall PTR, 2002
2. Stallings, W., .Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR., 2003
3. Stallings, W., .Network Security Essentials: Applications and Standards, Prentice Hall, 2000