St. Martin's Engineering College

UGC AUTONOMOUS
NBA & NAAC A+ Accredited
Dhulapally, Secunderabad-500 100

www.smec.ac.in

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE (AI & DS)

CRYPTOGRAPHY AND NETWORK SECURITY (Professional Elective – III)

IV B. TECH - I SEMESTER (R 22)

Course Code	Programme	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIE	SEE	Total
AID735PE	B. Tech	3	0	0	3	40	60	100

COURSE OBJECTIVES

To learn

- 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

COURSE OUTCOMES

Upon successful completion of the course, the student is able to

- 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:

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, plain text and cipher text, 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

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:

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

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

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, Cross site Scripting Vulnerability.

TEXT BOOKS

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

REFERENCE BOOKS

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw 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

WEB REFERENCES

1. https://www.geeksforgeeks.org/cryptography-and-network-security-principles/
2. https://www.scaler.com/topics/computer-network/cryptography-and-network-security/
3. https://www.codingninjas.com/studio/library/cryptography-and-network-security

E -TEXT BOOKS

1. https://in.bpbonline.com/products/cryptography-and-network-security
2. https://dl.acm.org/doi/10.5555/2523199
3. https://styluspub.presswarehouse.com/browse/book/9781683928836/Network-Security-and-Cryptography

MOOCS COURSE

1. https://www.coursera.org/courses?query=cryptography
2. https://www.udemy.com/topic/cryptography/
3. https://www.ucertify.com/exams/uCertify/CryptoSec.AB1.E1.html