PVP 23

PRASAD V. POTLURI SIDDHARTHA INSTITUTE OF TECHNOLOGY

(Autonomous)
Kanuru, Vijayawada-520007

DEPARTMENT OF Computer Science and Engineering (Data Science)
III B. Tech – II Semester
Cryptography & Network Security

Syllabus

Course Code	23DS4601B	**Year**	III	**Semester**	II
Course Category	PEC	**Branch**	CSE (Data Science)	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	Computer Networks
Continuous Internal Evaluation	30	**Semester End Evaluation**	70	**Total Marks**	100

Course Outcomes		
Upon Successful completion of course, the student will be able to		
CO1	Describe the foundational concepts of network security, classical encryption techniques, cryptographic principles, and modern cryptographic algorithms to understand principles of security	**L2**
CO2	Apply symmetric and asymmetric encryption techniques, hash functions, and message authentication codes to design secure communication systems.	**L3**
CO3	Use digital signature schemes and internet security protocols like IPsec and secure email mechanisms to ensure authentication and confidentiality in real-time applications.	**L3**
CO4	Analyze the effectiveness and security of cryptographic algorithms and network security protocols to address modern cybersecurity challenges.	**L4**

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations **(3: Substantial, 2: Moderate, 1: Slight)**

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PSO1**	**PSO2**
CO1	2												
CO2	3												
CO3	3												
CO4		3									2		

Syllabus		
Unit No	**Contents**	**Mapped CO**
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.	CO1
II	**Classical Encryption Techniques:** Symmetric cipher model, Substitution Techniques, Transposition Techniques. **Block Ciphers and Data Encryption Standard:** Traditional Block Cipher Structure, The Data Encryption Standard (DES), A DES Example, The Strength of DES, Block cipher design principles. **Advanced Encryption Standard:** AES Structure, AES Transformation Functions.	CO1, CO2, CO4
III	**Asymmetric key Ciphers:** Principles of public key cryptosystems, RSA algorithm, Diffie-Hellman Key Exchange, Elgamal Cryptographic system, Elliptic Curve Cryptography.	CO1, CO2, CO4
IV	**Cryptographic Hash Functions**: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithms (SHA) **Digital Signatures:** Digital Signatures, Elgamal Digital Signature Scheme, Elliptic Curve Digital Signature Algorithm.	CO1, CO3, CO4
V	**IP Security**: IP Security Overview, IP Security Policy, Encapsulating Security Payload. **Electronic-Mail Security:** Internet-mail Security, Email Format, Email Threats and Comprehensive Email Security, S/MIME.	CO1, CO3, CO4

Learning Resources
Text Books
1. Cryptography and Network Security: Principles and Practice, William Stallings, 7th Edition, 2017, Pearson Education. 2. Cryptography and Network Security, Behrouz A. Forouzan and Debdeep Mukhopadhyay, 3rd Edition, 2015, McGraw Hill.
References
1. Cryptography and Network Security, Atul Kahate,4th Edition, 2019, McGraw-Hill Education 2. Introduction to Cryptography with Coding Theory, Wade Trappe and Lawrence C,Washington,3rd Edition, 2020, Pearson 3. Modern Cryptography: Theory and Practice, 1st Edition, 2003, Pearson / Prentice Hall
E-Recourses and other Digital Material
1. https://nptel.ac.in/courses/106105162 2. https://onlinecourses.nptel.ac.in/noc22_cs90/preview 3. https://onlinecourses.nptel.ac.in/noc25_ee54/preview 4. https://onlinecourses.nptel.ac.in/noc22_cs03/preview

Course Coordinator:

Module Coordinator:

Program Coordinator: **HOD**