PRASAD .V. POTLURI SIDDHARTHA INSTITUTE OF TECHNOLOGY
(Autonomous)

Kanuru, Vijayawada-520007

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (AI & ML)

III B. Tech – II Semester CSE (AI&ML)

Cryptography and Network Security

Course Code	20AM3601	Year	III	Semester	II
Course Category	PCC	Branch	CSE (AI&ML)	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 fundamental principles of cryptography and network security.	**L2**
CO2	Apply symmetric and asymmetric cryptographic algorithms to encrypt and decrypt data.	**L3**
CO3	Apply cryptographic hash functions, digital signatures and authentication protocols to ensure data integrity and secure communication in practical scenarios.	**L3**
CO4	Analyze various encryption algorithms, hash functions and security protocols for their strengths and weaknesses and evaluate their applicability in different network security contexts.	**L4**

Contribution of Course Outcomes towards achievement of Program Outcomes& Strength of correlations (3: High,2: Medium, 1: Low)														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2													
CO2	3											1		
CO3	3											1		
CO4		3										2		

Syllabus		
Unit No	**Contents**	**Mapped CO**
I	**Security Fundamentals:** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Fundamental Security Design Principles, 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, AES Key Expansion, An AES Example.	CO1, CO2, CO4
III	**Public-key Cryptography:** Principles of public-key cryptosystems, The 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, Secure hash algorithm (SHA). **Digital Signatures**: Digital signatures, Elgamal Digital Signature Scheme, Schnorr Digital Signature Scheme, NIST Digital Signature Algorithm,	CO1, CO3, CO4
V	**E-mail Security:** Internet Mail Architecture, Email Formats, Emal Threats and Comprehensive Email Security**,** S/MIME, Pretty Good Privacy (PGP). **IP Security:** IP Security Overview, IP Security Policy, Encapsulating Security Payload.	CO1, CO4

Learning Resources
Text Books
1. Cryptography and Network Security Principles and practice by W. Stallings, Seventh Edition, 2017, Pearson Education.
References
1. Cryptography: Theory and Practice, Stinson. D. Third Edition , 2012, Chapman & Hall/CRC. 2. Cryptography and Network Security, Behrouz A. Forouzan and Debdeep Mukhopadhyay, Second Edition, 2013, Tata McGraw Hill . 3. Cryptography and Network Security, Atul Kahate, 2003, Tata McGraw-Hill .
E-Recourses and other Digital Material
1. https://archive.nptel.ac.in/courses/106/105/106105031/ 2. http://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles- and-practice-7th-global-edition.pdf 3. https://www.udemy.com/topic/network-security/