SWARNANDHRA
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)

Accredited by National Board of Accreditation, AICTE, New Delhi, Accredited by NAAC with "A" Grade – 3.32 CGPA, Recognized under 2(f) & 12(B) of UGC Act 1956, Approved by AICTE, New Delhi, Permanent Affiliation to JNTUK, Kakinada
Seetharampuram, W.G.DT., Narsapur-534280, (Andhra Pradesh)

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

TEACHING PLAN

Course Code	Course Title	Semester	Branch	Contact Periods /Week	Academic Year	Date of commencement of Semester
20CS7E01	Cryptography and Network Security	VII	AI&ML	5	2024-25	03-06-2024

Pre-requisites:	Computer Networks

COURSE OUTCOMES

1	Explain different security threats and counter measures and foundation course of cryptography mathematics[K2].
2	Classify the basic principles of symmetric key algorithms and operations of some symmetric key algorithms and asymmetric key cryptography[K2].
3	Revise the basic principles of Public key algorithms and Working operations of some Asymmetric key algorithms such as RSA, ECC and some more[K4].
4	Design applications of hash algorithms, digital signatures and key management techniques.[K3]
5	Determine the knowledge of Application layer, Transport layer and Network layer security Protocolssuch as PGP, S/MIME, SSL,TSL, and IPsec[K3].

Unit	Out Comes / Bloom's Level	Topics No.	Topics/Activity	Text Book / Reference	Contact Hour	Delivery Method
UNIT-I: Basic Principles						
I	CO1: Implement and Techniques based in security.	1.1.1	Security Goals	T1	1	Chalk ,talk
		1.1.2	Security Attacks,	T1	1	Chalk ,talk
		1.1.3	Security Services	T1	1	Chalk ,talk
		1.1.4	Algorithm analysis and complexity	T1	1	Chalk ,talk
		1.1.5	Security Mechanisms			
		1.1.6	Symmetric Cipher Model	T1	1	
		1.1.7	Substitution Techniques	T1	1	Chalk ,talk
		1.1.7	Transposition Technique	T1	1	PPT
		1.1.8	Phishing Measure	T1	1	Chalk, talk,PPT
		1.1.9	Defensive Measure	T1	1	PPT
		1.2.1	Web-Based Attacks,	T1	1	Web Resources

		1.2.2	Structured Query Language(SQL)	T1	1	PPT
		1.2.3	Implementing SQL	T1	1	NPTEL video
		1.2.4	Injection attacks	T1	1	Web Resources
Revision of Security and SQL					1	PPT
				Total	**16**	
UNIT-II: Traditional Block Cipher Structure						
II	CO2: Mechanism in Symmetric Encryption.	2.1.1	Symmetric Encryption	T2	1	Chalk ,talk
		2.1.2	Traditional Block Cipher Structure	T2	1	Web Resources
		2.2.1	Stream Cipher and Block Cipher.	T2	1	Chalk , talk
		2.2.2	Mathematics of Symmetric Key Cryptography	T2	1	Chalk ,talk
		2.2.3	Introduction to Modern SymmetricKey Ciphers	T2	1	Web Resources
		2.3.1	Data Encryption Standard	T2	1	Web Resources
		2.3.2	IDEA(International Data Encryption Algorithm)	T2	1	Chalk ,talk, ppt
		2.3.3	operations on IDEA	T2	1	PPT
		2.3.4	Applications of IDEA	T2	1	Web Resources
		2.3.5	Encryption Implementation	T2	1	Chalk ,talk
		2.3.6	Encryption Standard	T2	1	Web Resources
		2.3.7	Advanced Encryption Standard	T2	1	Web Resources
		Revision of Symmetric Encryption			1	PPT
Total					**13**	
UNIT-III: Asymmetric Encryption						
III	CO3: Mechanism in Asymmetric Encryption.	3.1.1	Mathematics of Asymmetric Key Cryptography	T1	1	Chalk ,talk
		3.1.2	Decryption Implementation	T1	1	Chalk ,talk, ppt
		3.1.3	Decryption standard	T1	1	Web Resources
		3.1.4	Operations on decryption key	T1	1	NPTEL video
		3.1.5	Asymmetric Key Cryptography	T1	1	PPT
		3.2.1	RSA Algorithm	T3	1	PPT
		3.2.2	Algorithm for Diffe-Hellman Key	T3	1	Web

			Exchange			Resources
		3.2.3	Elliptic Curve Cryptography	T3	1	Chalk ,talk
		Revision of Asymmetric Key Cryptography			1	PPT
				Total	9	
UNIT-IV: Data Integrity, Digital Signature Schemes & Key Management						
IV	CO4: Applications of Cryptographic Hash Function.	4.1.1	Data Integrity	T1	1	PPT
		4.1.2	Message Integrity Authentication	T1	1	Web Resources
		4.1.3	Message Authentication	T1	2	Chalk ,talk
		4.1.4	Hash Function	T1	1	PPT
		4.1.5	Applications of Cryptography Hash Functions	T1	1	Chalk ,talk
		4.1.6	SHA(Secure Hash Algorithm)	T1	1	Web Resources
		4.1.7	Digital Signature	T1	1	Web Resources
		4.1.8	Key Management	T3	1	Web Resources
		4.1.9	Distribution	T3	2	Web Resources
		4.2.0	Distribution Management	T3	2	Web Resources
Revision of Message Integrity					1	Chalk ,talk, ppt
				Total	14	
UNIT-V: Network Security-I						
V	CO5: Demonstrate the implementation of Authentication Principles.	5.1.1	Remote User Authentication Principles	T3	1	Web Resources
		5.1.2	Kerberos	T3	1	Chalk ,talk
		5.1.3	Web Security	T3	2	Chalk , talk PPT
		5.2.1	Security at application layer	T3	2	PPT
		5.2.2	PGP and S/MIME	T3	1	Web Resources
		5.2.3	SSLand TLS, Network	T3	2	Chalk ,talk
		5.3.1	Security at the Transport Layer	T3	1	Web Resources
		5.3.2	IPSec, System Security	T3	1	Chalk ,talk, ppt
Revision of Security at the Network Layer					1	PPT
				Total	12	
CUMULATIVE PROPOSED PERIODS					64	

Text Books:	
S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1.	Deb deep Mukhopadhyay, Cryptography and Network Security, 3rd Edition McGraw Hill,2015
2.	William Stallings,Cryptography and Network Security,4th Edition,(6e) Pearson,2006
3.	Keith M.Martin, ,Everyday Cryptography, 1st Edition, Oxford,2016
Reference Books:	
S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1.	Bernard Meneges, Network Security and Cryptography, 1st Edition, , Cengage Learning,2018
Web Details	
1.	https://www.tutorialspoint.com/cryptography/index.htm
2.	https://www.gatevidyalay.com/tag/cryptography-and-network-security-tutorial/
3.	https://www.geeksforgeeks.org/cryptography-introduction/
4.	https://www.vssut.ac.in/lecture_notes/lecture1428550736.pdf
5.	https://www.scaler.com/topics/computer-network/cryptography-and-network-security/

		Name	Signature with Date
i.	Faculty	K.Satyanarayana	
ii.	Course Coordinator	Dr.G.Sudhakar	
iii.	Module Coordinator	K.Jai Prakash	
iv.	Program Coordinator	Dr.B.Rama krishna	

Principal