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 COMPUTER SCIENCE AND ENGINEERING
TEACHING PLAN

Course Code	Course Title (Regulation)	Semester/ Sections	Branch	Contact Periods/ Week	Academic Year	Date of commencement of Semester
20CS7E01	Cryptography and Network Security (R20)	VII A, B, C, D &E	CSE	5	2025 - 26	09.06.2025

COURSE OUTCOMES
After completion of the course students are able to

CO 1	Apply different security threats, countermeasures and foundation course of cryptography mathematics. (K3)
CO 2	Classify basic principles of symmetric key algorithms and operations of some symmetric key algorithms and asymmetric key cryptography (K2)
CO 3	Restate basic principles of public key algorithms and Working operations of some Asymmetric key algorithms (K)
CO 4	Show applications of hash algorithms, digital signatures and key management techniques(K3)
CO 5	Determine the knowledge of Application layer, Transport layer and Network layer security Protocols(K3)

Unit No	Out Comes / Bloom's Level	Topics No.	Topics/Activity	Text Book/ Reference	Contact Hour	Delivery Method
1	<u>CO1.:</u> Apply different security threats, countermeasures and foundation course of cryptography mathematics. (K3)	**Unit-1: Introduction**				
		1.1	**Basic Principles:** Security Goals	T1	1	Chalk & Talk, PPT
		1.2	Security Attacks	T1	1	
		1.3	Security Services	T1	1	
		1.4	Security Mechanisms	T1	1	
		1.5	**Basics of Cryptography:** Symmetric Cipher Model	T1	1	
		1.6	Substitution Techniques	T1	2	
		1.7	Phishing and Defensive Measure	T1	2	
		1.8	Web-Based Attacks	T1	1	
		1.9	Structured Query Language (SQL) Injection attacks	T1	1	
		1.10	Content beyond	T1	1	
		1.11	Class Test	T1	1	
				Total	**13**	
2		**Unit-2: Traditional Block Cipher Structure**				
		2.1	Stream Cipher and Block Cipher)	T1	2	

	CO2. Classify basic principles of symmetric key algorithms and operations of some symmetric key algorithms and asymmetric key cryptography (K2)	2.2	**Symmetric Encryption:** Mathematics of Symmetric Key Cryptography	T1	2	Chalk & Talk, PPT
		2.3	Introduction to Modern Symmetric Key Ciphers	T1	2	
		2.4	Data Encryption Standard	T1	2	
		2.5	IDEA (International Data Encryption Algorithm)	T1	2	
		2.6	Advanced Encryption Standard.	T1	2	
		2.7	Content beyond	T1	1	
		2.8	Class Test	T1	1	
				Total	**14**	
3	**CO 3.** Restate basic principles of public key algorithms and Working operations of some Asymmetric key algorithms (K2)	**Unit-3: Asymmetric Encryption**				
		3.1	Mathematics of Asymmetric Key Cryptography	T1	3	Chalk & Talk, PPT
		3.2	Asymmetric Key Cryptography	T1	2	
		3.3	RSA Algorithm	T1	2	
		3.4	Diffie-Hellman Key Exchange	T1	2	
		3.5	Elliptic Curve Cryptography	T1	2	
		3.6	Content beyond	T1	1	
		3.7	Class Test	T1	1	
				Total	**13**	
MID I EXAMINATIONS						
4	**CO 4.** Show applications of hash algorithms, digital signatures and key management techniques(K3)	**Unit-4: Data Integrity, Digital Signature Schemes & Key Management**				
		4.1	Hash Function	T1	2	Chalk & Talk, PPT
		4.2	Applicationsof Cryptographic Hash Functions	T1	1	
		4.3	SHA (Secure Hash Algorithm)	T1	1	
		4.4	Message Integrity and Message Authentication	T1	2	
		4.5	Digital Signature	T1	2	
		4.6	Key Management and Distribution.	T1	2	
		4.7	Content beyond	T1	1	
		4.8	Class Test	T1	1	
				Total	**12**	
5	**CO 5.** Determine the knowledge of Application layer, Transport layer and Network layer security Protocols(K3)	**Unit 5: Network Security-I&II**				
		5.1	Remote User Authentication Principles	T1	1	Chalk & Talk, PPT
		5.2	Kerberos	T1	1	
		5.3	Web Security	T1	1	
		5.4	Securityat application layer: PGP	T1	1	

		5.5	S/MIME	T1	1	
		5.6	Security at the Transport Layer: SSL	T1	1	
		5.7	TLS	T1	1	
		5.8	Secure Shell (SSH),	T1	1	
		5.9	Security at the Network Layer: IPSec	T1	1	
		5.10	System Security	T1	1	
		5.11	Content beyond	T1	1	
		5.12	Class Test	T1	1	
				Total	**12**	
CUMULATIVE PROPOSED PERIODS					**64**	
MID II EXAMINATIONS						
END EXAMINATIONS						

Text Books		
Sl. No.	**AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION**	
1	T1	Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deepMukhopadhyay, McGraw Hill,2020
2	T2	Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2018
3	T3	Everyday Cryptography, 1st Edition, Keith M. Martin, Oxford,2018
Reference Books		
1	R1	Network Security and Cryptography, 1st Edition, Bernard Meneges, CengageLearning,2018

		Name	Signature with Date
i.	Faculty-I	Dr.P. Srinivasulu	
ii.	Course Coordinator Faculty-II	Dr P. Pandarinath	
iii.	faculty -III	Dr S. Gopinath	
iv.	faculty -IV	Mr M. Satyanarayana	
v.	faculty -V	Mr K. Rajesh Kumar	
vi.	Module Coordinator	Mr K.Rajesh Kumar	
vii.	Programme Coordinator	Dr.P.Srinivasulu	

PRINCIPAL