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 INFORMATION TECHNOLOGY
TEACHING PLAN

Course Code	Course Title	Semester	Branch	Contact Periods /Week	Academic Year	Date of commencement of Semester
20CC6T01	CRYPTOGRAPHY AND NETWORK SECURITY	VI	CSE & BS	6	2024-2025	18-11-2024

COURSE OUTCOMES

1	Explain different security threats and countermeasures and foundation course of cryptography mathematics.
2	Classify the basic principles of symmetric key algorithms and operations of somesymmetric key algorithms and asymmetric key cryptography
3	Revise the basic principles of Public key algorithms and Working operations ofsome Asymmetric key algorithms such as RSA, ECC and some more
4	Design applications of hash algorithms, digital signatures and key managementtechniques
5	Determine the knowledge of Application layer, Transport layer and Networklayer security Protocols such as PGP, S/MIME, SSL,TSL, and IPsec .

UNIT	Out Comes / Bloom's Level	Topics No.	Topics/ Activity	Text Book/ Reference	Contact Hour	Delivery Method
I	CO – 1	1.1	Security Goals Security Attacks	T2	1	Chalk & Board
		1.2	Security Services	T2	1	
		1.3	Security Mechanisms	T2	1	
		1.4	Symmetric Cipher Model	T2	1	Power point presentation
		1.5	Substitution Techniques	T2	2	
		1.6	Transportation Techniques	T2,T1	2	
		1.7	Phishing and Defensive Measure	T2,T1	1	Assignment
		1.8	Web-Based Attacks	T2,T1	1	
		1.9	Structured Query Language (SQL) Injection attacks.	T2,T1	2	Test
				Total	12	
II	CO – 2	2.1	Stream Cipher and Block Cipher	T1	2	Chalk & Board
		2.2	Mathematics of Symmetric Key Cryptography	T1	2	
		2.3	Introduction to ModernSymmetric Key Ciphers	T1	1	
		2.4	Data Encryption Standard	T1	2	Power point presentation
		2.5	IDEA(International Data Encryption Algorithm)	T1	2	
		2.6	Advanced Encryption Standard	T1	2	Assignment

Content beyond syllabus		**2.7**	Blowfish Algorithm	**T1**	**1**	Test
				Total	**12**	
III	**CO - 3**	**3.1**	Mathematics of Asymmetric Key Cryptography	**T1,R1**	**2**	**Chalk & Board**
		3.2	Fermat's and Euler's Theorems	**T1,R1**	**2**	
		3.3	Chinese Remainder Theorem	**T1,R1**	**2**	**Power point presentation**
		3.4	Asymmetric Key Cryptography	**T1,R1**	**2**	
		3.5	RSA Algorithm	**T1,T2**	**2**	
		3.6	Diffie-Hellman Key Exchange	**T1,T2**	**2**	**Assignment**
		3.7	Introduction to Elliptic Curve Cryptography	**T1,T2**	**2**	**Test**
				Total	**14**	
IV	**CO – 4**	**4.1**	**Cryptographic Hash Functions:** Applications of Cryptographic Hash Functions	**T1**	**2**	**Chalk & Board**
		4.2	Secure Hash Algorithm	**T1**	**2**	**Power point presentation**
		4.3	Message Integrity	**T1**	**2**	
		4.4	Message Authentication	**T1**	**2**	
		4.5	Digital signatures	**T1**	**2**	**Assignment**
		4.6	Key Management and Distribution.	**T1**	**2**	**Test**
				Total	**12**	
V	**CO – 5**	**5.1**	Remote User Authentication	**T1,R1**	**1**	**Chalk & Board**
		5.2	Kerberos	**T1,R1**	**2**	
		5.3	Web Security	**T1,R1**	**2**	
		5.4	Securityat application layer: PGP	**T1,R1**	**2**	
		5.5	S/MIME	**T1,R1**	**2**	
		5.6	Security at the Transport Layer: SSLand TLS,	**T1,R1**	**2**	**Power point presentation**
		5.7	Secure Shell(SSH)	**T1,R1**	**1**	
		5.8	Security at the Network Layer: IPSec	**T1,R1**	**1**	**Assignment**
		5.9	System Security	**T1,R1**	**1**	**Test**
Content beyond syllabus		**5.10**	Electronic Mail Security	**T1,R1**	**1**	
				Total	**15**	
				CUMULATIVE PROPOSED PERIODS	**65**	

Text Books:

S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1	Behrouz A. Fourouzan and Debdeep Mukhopadhyay, Cryptography and Network, 3rd

	Edition, McGraw-Hill, 2015.
2	William Stallings , Cryptography and Network Security: Principles and Practice, 5th Edition, Pearson Education, 2011.
3	Keith M. Martin, Everyday Cryptography,1st Edition, Oxford,2016

Reference Books:

S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1	Bernard Menezes, Network Security and Cryptography, Cengage Learning, 2011

Web Details:

1	**https://www.geeksforgeeks.org/cryptography-introduction/**
2	https://www.brainkart.com/article/Cryptography-and-Network-Security--Introduction_8336/
3	**https://www.tutorialspoint.com/ cryptography.**
4	ttps://www.javatpoint.com/ Cryptography-and-Network-Security

		Name	Signature with Date
i.	Faculty	Mr. K.Bhanu Chand	K Bhanu
ii.	Module Coordinator	Mr. K.Bhanu Chand	K Bhanu
iii.	Programme Coordinator	Dr. RVVSV Prasad	

Principal