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	Semester	Branches	Contact Periods /Week	Academic Year	Date of commencement of Semester
16CS7T02	Cryptography and Network Security	VII	CSE A,B,Shift	5	2020-21	

COURSE OUTCOMES:

1	Illustrate the different type of Security attacks(K2)
2	Analyze and compare Security Mechanisms and Services(K4)
3	Demonstrate mathematical foundations required for Cryptographic Algorithms(K3)
4	Distinguish different modern Encryption Algorithms (K2)
5	Define the basic Knowledge in different Authentication Mechanisms(K1)
6	Justify latest techniques used in different Security aspects (Ex. Network Security and Web Security etc.)(K4)

Unit	Out Comes / Bloom's Level	Topics No.	Topics/Activity	Text Book / Reference	Contact Hour	Delivery Method
UNIT-I: Introduction & Basics of Cryptography						
I	CO1: Illustrate the different type of Security attacks(K2)	1.1	**Introduction:** Security Attacks	T1	1	Chalk ,talk
		1.2	Security Services	T1	1	PPT
		1.3	Security Mechanisms	T1	1	Web Resources
		1.4	Model for Network Security	T1	1	NPTEL video
		1.5	**Basics of Cryptography**: Symmetric Cipher Model	T2	1	Chalk ,talk
		1.6	Substitution Techniques	T2	1	PPT
			Examples		1	Web Resources
		1.7	Transposition Techniques	T2	1	Chalk ,talk PPT
			Examples	T2	1	Web Resources
	Content beyond Syllabus (if needed)		Functional encryption		1	PPT
				Total	**10**	

UNIT-II: Secret Key Cryptography						
II	CO2: Analyze and compare Security Mechanisms and Services(K4)	2.1	**Secret Key Cryptography:** Data Encryption Standards (DES)	T1	1	Chalk ,talk
		2.2	Strength of DES	T1	1	Web Resources
		2.3	Block Cipher Design Principles	T1	1	Chalk , talk
		2.4	Modes of Operations	T1	1	Chalk ,talk
		2.5	Triple DES	T1	1	Web Resources
			Example for Triple DES	T1	1	PPT
		2.6	Blowfish	T1	1	Web Resources
			Example for Blowfish	T1	1	PPT
		2.7	AES	T1	1	Chalk ,talk, ppt
			Example for AES	T1	1	PPT
	Content beyond Syllabus (if needed)		lattice-based cryptography, and foundations		1	Chalk ,talk
Total					**11**	
UNIT-III: Number Theory						
III	CO3: Demonstrate mathematical foundations required for Cryptographic Algorithms(K3)	3.1	**Number Theory:** Prime and Relatively Prime Numbers	R1	1	Chalk ,talk
		3.2	Modular Arithmetic	R1	1	Chalk ,talk,
		3.3	Example for Modular Arithmetic	R1	1	NPTEL video
		3.4	Fermats and Euler's Theorem	R1	1	PPT
		3.5	Example for Fermats and Euler's Theorem	T2	1	PPT
		3.6	The Chinese Remainder Theorem	T1	1	Chalk , talk
		3.7	Example for Chinese Remainder Theorem	T1	1	Chalk ,talk
		3.8	Discrete Logarithms	T1	1	Web Resources
		3.9	Example for Discrete Logarithms	T1	1	Web Resources
	Content beyond Syllabus (if needed)		stegonagraphy		1	Chalk ,talk
Total					**10**	
UNIT-IV: Public Key Cryptography						
IV	CO4: Distinguish	4.1	Introduction to **Public Key Cryptography**	T1	2	PPT
			Principles of Public Key	T1		PPT

	different modern Encryption Algorithms (K2)		Cryptosystems			
		4.2	RSA Algorithm Introduction	T1	1	PPT
			Example for RSA Algorithm	T1	1	PPT
		4.3	Diffie- Hellman Key Exchange Introduction	T1	1	Chalk ,talk
			Example 1 for Diffie- Hellman Key Exchange	T1	1	PPT
			Example 2 for Diffie- Hellman Key Exchange	T1	1	Chalk ,talk
		4.4	Introduction to Elliptive Curve Cryptography	T1	1	PPT
			Example for Elliptive Curve Cryptography	T1	1	Web Resources
		4.5	Overview of **Public Key Cryptography**	T1	1	Web Resources
	Content beyond Syllabus (if needed)	**Elliptic-curve cryptography (ECC)**			1	Chalk ,talk, ppt
				Total	**11**	
UNIT-V: Cryptographic Hash Functions						
V	CO5: Define the basic Knowledge in different Authentication Mechanisms(K1)	5.1	Secure Hash Algorithm	T1	1	Web Resources
		5.2	Message Authentication Codes: Message Authentication Requirements and Functions	T1	1	Web Resources,
		5.3	HMAC	T1	1	Chalk ,talk, ppt
		5.4	Digital Signatures	T1	1	PPT
		5.5	digital signature process	T1	1	Chalk ,talk
		5.6	Digital Signature Schemes	T1	1	PPT
		5.7	Digital Signature Standards	T1	1	PPT
		5.8	digital signature types	T1	1	Web Resources
			5.8.1 Direct digital signature	T1	1	Chalk ,talk
			5.8.2 Arbitrated digital signature	T1	1	Chalk ,talk
			Example for digital signature	T1	1	PPT
	Content beyond Syllabus (if needed)	quantum cryptography			1	Chalk ,talk, PPT
				Total	**12**	

UNIT-VI: IP Security,Web Security & **System Security**						
VI	CO6: Justify latest techniques used in different Security aspects (Ex. Network Security and Web Security etc.)(K4)	6.1	Architecture	T1	1	Web Resources
		6.2	Authentication Header, Encapsulating Security Payload	T1	1	NPTEL videos
		6.3	**Web Security:**Web Security Considerations,	T1	1	Chalk ,talk, ppt
		6.4	Secure Socket Layer.	T1	1	PPT
		6.5	Transport Layer Security	T2	1	Web Resources
		6.6	**System Security:** Intruders, Intrusion Detection	T2	1	Chalk ,talk
		6.7	Password Management	T2	1	Web Resources
		6.8	Malicious Software-Types Viruses	T1	1	PPT
		6.9	Virus Counter measurements, Worms	T2	1	Web Resources
		6.10	Firewalls-Characteristics	T2	1	Chalk ,talk
		6.11	Types of Firewall	T2	1	Web Resources
	Content beyond Syllabus (if needed)	lattice-based cryptography, and foundations			1	PPT
				Total		**12**
				CUMULATIVE PROPOSED PERIODS		**66**

Text Books:	
S.No.	**AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION**
1	William Stallings,Cryptography & Network Security: Principles and Practices,Sixth edition, PEA-2019.
2	Chwan Hwa Wu, J.David Irwin,Introduction to Computer Networks & Cyber Security, 1st edition, CRC press-2017
3	Ryan Russell, Hack Proofing your Network, 2nd edition, Kaminsky, Forest Puppy, Wiley Dreamtech-2012.
Reference Books:	
S.No.	**AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION**
1	Keith Martin, Everyday Cryptography, Fundamental Principles & Applications, 2nd edition, Oxford-2017
2	Bernard Menezes,Network Security & Cryptography, 2nd edition, Cengage-2010
Web Details	
1	williamstallings.com/Extras/Security-Notes/
2	cs.brown.edu/courses/csci1510/.../goldwasser_bellare_notes.pdf
3	www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/
4	freevideolectures.com › Computer Science › IIT Kharagpur

		Name	Signature with Date
i.	Faculty	Mr. P.RAVI KIRAN/Assoc.Professor	
ii.	Course Coordinator	Mr. P.RAVI KIRAN/Assoc.Professor	
iii.	Module Coordinator	Mr. P.RAVI KIRAN/Assoc.Professor	
iv.	Programme Coordinator	Dr.P.Srinivasulu/ Professor	

Principal