

SWARNANDHRA

COLLEGE OF ENGINEERING AND TECHNOLOGY (AUTONOMOUS)

SEETHARAMPURAM, NARSAPUR-534280, WG- DT, AP

DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS

TEACHING PLAN

Course Code	Course Title	Year/Sem	Branch	Contact Hrs/Week	Academic Year
24MC2T02	Network Security and Cyber Security	I/II	MCA	6	2025-2026

COURSE OUTCOMES (CO): Students are able to

1. Explain basic cryptography principles, including security goals, attacks, and symmetric Encryption techniques like DES and AES. (K2)
2. Apply asymmetric encryption methods and compare cryptographic has functions such as SHA and SHA-3. (K3)
3. Analyze digital signature schemes and evaluates security measures for email and IP security. (K4)
4. Identify and classify cybercrimes and understand the roles and motivations of cybercriminals. (K1)
5. Evaluate advanced cyber threats and propose security measures to counter them. (K5)

Unit	Outcome/ Blooms Level	TOPIC/ACTIVITY		Text Books	Contact HOURS	Delivery Method
I	Explain basic cryptography principles, including security goals, attacks, and symmetric Encryption techniques like DES and AES (K2)	UNIT-I Basic Principles				Chalk & Board & Demonstration of Cryptographic Algorithms
		1.1	Basic Principles: Security Goals, Cryptographic Attacks	T1	1	
		1.2	Services and Mechanisms	T1	1	
		1.3	Mathematics of Cryptography	T1	2	

		1.5	Symmetric Encryption: Mathematics of Symmetric Key Cryptography	T1	2	
		1.6	Introduction to Modern Symmetric Key Ciphers	T1	1	
		1.7	Data Encryption Standard	T1	2	
		1.8	Advanced Encryption Standard	T1	2	
		UNIT-II Asymmetric Encryption				
II	Apply asymmetric encryption methods and compare cryptographic has functions such as SHA and SHA-3. (K3)	2.1	Mathematics of Asymmetric Key Cryptography	T1	1	Chalk & Board & Demonstration of Cryptographic algorithms
		2.2	Primes, Primality Testing, Factorization	T1	2	
		2.3	Asymmetric Key Cryptography	T1	1	
		2.4	RSA Cryptosystem	T1	1	
		2.5	Rabin Cryptosystem	T1	1	
		2.6	ElGamal Cryptosystem	T1	1	
		2.7	Elliptic Curve Cryptosystem	T1	1	
		2.8	Cryptographic Hash Functions: Applications of Cryptographic Hash Functions	T1	2	
		2.9	Two Simple Hash Functions	T1	1	
		2.10	Requirements and Security	T1	1	
		2.9	Hash Functions Based on Cipher Block Chaining	T1	1	
		2.10	Secure Hash Algorithm (SHA)	T1	1	
		2.11	SHA-3	T1	1	
III	Analyze digital signature schemes and evaluates security measures for email and IP security. (K4)	UNIT-III Digital Signatures				Chalk & Board & Demonstration of Cryptographic Algorithms
		3.1	ElGamal Digital Signature Scheme	T1	1	
		3.2	Schnorr Digital Signature	T1	1	
		3.3	NIST Digital Signature Algorithm	T1	2	
		MID EXAM-1				
		3.4	Electronic Mail Security: Internet Mail Architecture	T1	1	
		3.5	Email Formats	T1	1	
		3.6	Email Threats and Comprehensive Email Security	T1	1	
		3.7	S/MIME. IP Security: IP Security Policy	T1	2	
		3.8	Encapsulating Security Payload	T1	1	
		3.9	Combining Security Associations	T1	1	
		3.10	Internet Key Exchange	T1	1	

IV	Identify and classify cybercrimes and understand the roles and motivations of cybercriminals(K1)	UNIT-IV Introduction to Cybercrime				Chalk & Board PPT with Video Demonstration
		4.1	Introduction to Cybercrime: Introduction	T2	1	
		4.2	Cybercrime: Definition and Origins of the Word	T2	1	
		4.3	Cybercrime and Information Security	T2	1	
		4.4	Cybercriminals	T2	1	
		4.5	Classifications of Cybercrime	T2	2	
		4.6	Cyber Stalking	T2	1	
		4.7	Cyber Café and Cybercrimes	T2	1	
		4.8	Botnets	T2	1	
		4.9	Attack Vector	T2	1	
		4.10	Proliferation of Mobile and Wireless Devices	T2	2	
		4.11	Security Challenges Posed by Mobile Devices	T2	1	
		4.12	Attacks on Mobile/Cell Phones.	T2	1	
V	Evaluate advanced cyber threats and propose security measures to counter them. (K5)	UNIT-V Proxy Servers and Anonymizers				Chalk & Board PPT with Video Demonstration
		5.1	Proxy Servers and Anonymizers	T2	1	
		5.2	Phishing, Password Cracking	T2	1	
		5.3	Keyloggers and Spywares	T2	1	
		5.4	Viruses and Worms	T2	1	
		5.5	Trojan Horses and Backdoors	T2	1	
		5.6	Steganography, Sniffers	T2	2	
		5.7	Spoofing, Session Hijacking	T2	1	
		5.8	Buffer Overflow, DoS and DDoS Attacks	T2	1	
		5.9	SQL Injection, Buffer Overflow	T2	1	
		5.10	Attacks on Wireless Networks	T2	1	
		5.11	Identity theft, Foot printing and Social Engineering	T2	1	
		5.12	Port Scanning, Email Investigation	T2	2	
		5.13	E-Mail Tracking, IP Tracking	T2	1	
		5.14	Email Recovery	T2	1	
		5.15	Password Cracking.	T2	1	

Course Beyond Syllabus		Impact of IOT on Cyber Security.	Web Resources	1	
MID EXAM 2					
TOTAL CLASSES			69		

Recommended Text Books for Reading:

1. Cryptography and Network Security, 3rd Edition, Behrouz A. Forouzan, Deb deep Mukhopadhyay, McGraw Hill, 2015.
2. SunitBelapure, Nina Godbole "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives," WILEY, 2011

Reference Text Books:

1. Network Security and Cryptography, First Edition, Bernard Menezes, Cengage Learning, 2018.
2. Cryptography and Network Security, William Stallings, Global Edition, 7e Pearson, 2017.

WEB RESOURCES:

1. <https://archive.nptel.ac.in/courses/106/105/106105162/>
2. <https://ebooks.inflibnet.ac.in/csp11/chapter/introduction-to-network-security/>
3. <https://www.fortinet.com/resources/cyberglossary/what-is-cryptography>
4. <https://ischoolonline.berkeley.edu/cybersecurity/curriculum/cryptography/>
5. <https://www.mitel.com/articles/web-communication-cryptography-and-network-security>
6. <https://www.nist.gov/cybersecurity>
7. <https://www.codecademy.com/learn/introduction-to-cybersecurity>


Faculty


Head of the Department


Principal