PARVATHANENI BRAHMAYYA SIDDHARTHA COLLEGE OF ARTS & SCIENCE
Autonomous
Siddhartha Nagar, Vijayawada-520010
Re-accredited at 'A+'by the NAAC

Offered to: M.C.A

22CA4E2: CYBER SECURITY

CourseDescriptionandPurpose: Tounderstand the field of computer security, threats, hardening systems, securing networks, cryptography and organizational security policies and how to protect computer operating systems, networks, and data from cyber-attacks and how to monitor systems and mitigate threats when they happen.

Course Objective: Course aim isto equip students with the technical knowledge and skills needed to protect and defend computer systems and networks. To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.

Course Outcomes:
On successful completion the students should be able to
CO1: Recall the concepts ofComputer andNetwork Security.
CO2: Demonstrate the ClassicalEncryption Techniques, application of Public Key Cryptography, RSA, and Message
Authentication Codes, AES,KeyManagement, financial frauds.
CO3: Plan an introduction to Cybercrime and criminals,Cyber offenses .
CO4: AnalyzeCyber offenses**,** mobile and wireless devices, along with tools and methods used in Cybercrime.
CO5: Perceive cybercrime handheld device forensics in Cybercrime, using illustrations, examples, and mini-cases.

CO-PO MATRIX							
COURSE CODE	**CO-PO**	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**
	CO1	H	H				
	CO2	H		M			
	CO3	H			L		
	CO4		H				
	CO5	M					L

UNIT-I (12 Hours)

ComputerandNetworkSecurityConcepts: ComputerSecurityConcepts-TheOSISecurityArchitecture-SecurityAttacks-SecurityServices-SecurityMechanisms-AModelfor NetworkSecurity.**ClassicalEncryptionTechniques:**SymmetricCipherModel-SubstitutionTechniques-TranspositionTechniques-RotorMachines - Steganography.**AdvancedEncryptionStandard:**AESStructure -AESTransformationFunctions - AESKeyExpansion-AnAESExample.

UNIT-II (12 Hours)

PublicKeyCryptographyandRSA: PrinciplesofPublicKey Crypto Systems-TheRSAAlgorithm.**KeyManagement:**OtherPublicKeyCryptoSystems:DiffieHellmanKeyExchange,ElgamalCryptographicSystem, EllipticCurve Arithmetic,Elliptic

CurveCryptography.**MessageAuthenticationCodes:** AuthenticationRequirements-AuthenticationFunctions-MessageAuthenticationCodes.

UNIT-III (12 Hours)

Introduction to Cybercrime: Introduction - Cybercrime: Definition and Origins of the Word -Cybercrimeand Information Security - Who are Cybercriminals? - Classifications of Cybercrimes - Cybercrime: TheLegal Perspectives - Cybercrimes: An Indian Perspective - Cybercrime and the Indian ITA 2000 - A GlobalPerspectiveonCybercrimes-CybercrimeEra:SurvivalMantrafortheNetizens-ConcludingRemarksandWayForwardtoFurther Chapters. **Cyberoffenses:HowCriminalsPlanThem:**Introduction-HowCriminals Plan theAttacks-SocialEngineering -Cyberstalking -Cybercafe and Cybercrimes -Botnets: The Fuel for Cybercrime - AttackVector- CloudComputing

UNIT-IV (12 Hours)

Cybercrime: Mobile and Wireless Devices: Introduction - Proliferation of Mobile and Wireless -Devices -Trends in Mobility- CreditCard Fraudsin Mobile and Wireless Computing Era - Security ChallengesPosed by Mobile Devices -Registry Settings for Mobile Devices - Authentication Service Security -Attacks on Mobile/Cell Phones - Mobile Devices: Security Implications for Organizations - OrganizationalMeasuresforHandlingMobile-OrganizationalSecurityPolicies andMeasures inMobileComputingEra-Laptops.**Tools and Methods Used in Cybercrime:** Introduction -Proxy Servers and Anonymizers - Phishing - Password Cracking - Keyloggers and Spywares - Virus and Worms - Trojan Horses and Backdoors -Steganography -DoSandDDoSAttacks -SQLInjection-BufferOverflow-AttacksonWirelessNetworks.

UNIT-V (12 Hours)

Forensics of Hand Held Devices: Introduction - Understanding Cell Phone Working Characteristics -Hand Held Devices and Digital Forensics - Toolkits for Hand-Held Device Forensics - Hunting threats withPandas - MFT Analysis -Extracting Feature Vectors From URL Strings For Malicious URL Detection -MonitorActive SSH Sessions WithPrometheusandGrafana.

Cybercrime: Illustrations, Examples and Mini Cases: Introduction - Real Life Examples - Mini Cases -Illustrations of Financial Frauds in Cyber Domain - Digital Signature - Related Crime Scenarios - DigitalForensicsCaseIllustrations- OnlineScams.

PrescribedTextBook			
	Author	Titl e	Publisher
1	WilliamStallings	CryptographyandNetworkSecurity	Pearson,SeventhEdition,2017
2	Nina Godbole,Sunit Belapur	CyberSecurityUnderstandingCyberCrimes,ComputerForensicsandLegalPerspectives	WileyIndiaPublications,Second EditionApril,2011
ReferenceTextBook			
	Author	Title	Publisher
1	WilliamStallings	NetworkSecurityEssentials-ApplicationsandStandards	PearsonEducation(2007),Third Edition.
2	ChrisMcNab	NetworkSecurityAssessment	OReilly (2007),2nd Edition
3	JonErickson	Hacking-TheArtofExploitation	Press(2006),SPD
4	NealKrawety	IntroductiontoNetworkSecurity	Thomson(2007)
5	AnkitFadia	NetworkSecurity-AHackersPerspective	Macmillan(2008)

PARVATHANENI BRAHMAYYA SIDDHARTHA COLLEGE OF ARTS & SCIENCE
Autonomous
Siddhartha Nagar, Vijayawada-520010
Re-accredited at 'A+'by the NAAC

M.C.A **Semester :IV**

Course Code: 22CA4E2 Course Name: Cyber Security

Time: 3 Hours **Max Marks: 70**

SECTION-A

Answer the following questions. (5×4=20Marks)

1. (a) Explain Security Attacks and its types (CO1,L2)
(or)
(b) Explain Steganography (CO1,L2)

2. (a) What is Encryption and Decryption? (CO2,L1)
(or)
(b) What is Cryptology? (CO2,L1)

3. (a) What are Authentication Requirements?(CO2,L1)
(or)
(b) What phishing and its working? (CO3,L1)

4. (a) Explain Keyloggers and its types (CO4,L2)
(or)
(b) Explain Cybercrime and who are cyber criminals (CO3,L2)

5. (a) What is Botnet? (CO5,L1)
(or)
(b) What is Cyber Terrorism? (CO5,L1)

SECTION-B

Answer the following questions. **(5×10=50Marks)**

6. (a) Explain Model for Network Security in detail with neat Diagram.(CO1,L2)
(b) Explain Transposition and Rotor Machine Technique in detail with example.(CO1,L2)
(or)
(c) Explain AES Cipher Encryption in detail.(CO2,L2)
7. (a) Apply RSA Algorithm for message authentication. (CO2,L3)
(or)
(b) Build Diffie Hellman Key Exchange with example. (CO2,L3)
8. (a) What are different ways of password cracking? (CO4,L1)
(or)
(b) What is SQL injection and what are the preventive measures from attack? (CO4,L1)
9. (a) Explain MonitorActive SSH Sessions WithPrometheusandGrafana.(CO4,L2)
(or)
(b) ExplainHunting threats with pandas. (CO5,L2)
10 (a) Plan the counter measures to be practiced for possible attacks on mobile/cell phones. (CO5, L5)
(or)
(b) Discuss how Keylogger be used to commit a cybercrime. (CO4,L5)
(c) Discuss DoS and DDoS in detail. (CO4,L5)