VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY HYDERABAD

B.TECH. MINOR IN CYBER SECURITY

COURSE STRUCTURE AND SYLLABUS

(Applicable for the batches admitted from the academic year 2022-2023)

V SEMESTER **R22**

Course Code	Title of the Course	L	T	P/D	CH	C
22MC1CY301	Principles of Information Security	3	0	0	3	3
22MC2CY301	Principles of Information Security Laboratory	0	0	3	3	1.5
Total		**3**	**0**	**3**	**6**	**4.5**

VI SEMESTER **R22**

Course Code	Title of the Course	L	T	P/D	CH	C
22MC1CY302	Foundations of Cyber Security	3	1	0	4	4
Total		**3**	**1**	**0**	**4**	**4**

VII SEMESTER **R22**

Course Code	Title of the Course	L	T	P/D	CH	C
22MC1CY401	Ethical Hacking	3	0	0	3	3
22MC1CY402	Digital Forensics					
22MC2CY401	Ethical Hacking Laboratory	0	0	3	3	1.5
22MC2CY402	Digital Forensics Laboratory					
Total		**3**	**0**	**3**	**6**	**4.5**

VIII SEMESTER **R22**

Course Code	Title of the Course	L	T	P/D	CH	C
22MC1CY403	Security Incident and Response Management	3	0	0	3	3
22MC1CY404	Mobile Security					
22MC1CY405	IoT Security					
22MC1CY406	Blockchain Technologies					
22MC1CY407	Authentication Techniques Cloud Security					
22MC4CY401	Mini – Project	0	0	4	4	2
22MC1CY402		**3**	**0**	**4**	**7**	**5**

L – Lecture T – Tutorial P – Practical D – Drawing CH – Contact Hours/Week

C – Credits SE – Sessional Examination CA – Class Assessment ELA – Experiential Learning Assessment

SEE – Semester End Examination D-D – Day to Day Evaluation LR – Lab Record

CP – Course Project PE – Practical Examination

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) V Semester

(22MC1CY301) PRINCIPLES OF INFORMATION SECURITY

TEACHING SCHEME		
L	T/P	C
3	0	3

EVALUATION SCHEME				
SE	CA	ELA	SEE	TOTAL
30	5	5	60	100

COURSE OBJECTIVES:

- To understand computer networks, security attacks, services, and mechanisms
- To describe various cryptosystems - symmetric key cryptography and public key cryptography
- To apply authentication services, mechanisms, and secure hash algorithms
- To be familiar with the concepts of email security, IDS, SSL, TLS, viruses, and Firewalls

COURSE OUTCOMES: After completion of course, the students should be able to

CO-1: Analyse the concepts of computer networks, cryptography, information security and its applications

CO-2: Build a security model to prevent and detect the attacks using various mechanisms

CO-3: Examine the authenticity of the messages, communicate securely and investigate non-repudiation

CO-4: Apply the concepts of SSL, TLS, firewalls and establish trusted systems

UNIT – I:

Defining Artificial Intelligence, Defining AI techniques, Using Predicate Logic and Representing Knowledge as Rules, Representing simple facts in logic, Computable functions and predicates, Procedural vs Declarative knowledge, Logic Programming.

UNIT – II:

Integer Arithmetic, Modular Arithmetic, Traditional Symmetric Key Ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES).

UNIT – III:

Mathematics of Cryptography: Primes, Primality Testing, Factorization, Chinese Remainder Theorem, Asymmetric Cryptography: Introduction, RSA Cryptosystem, Rabin Cryptosystem, Elliptic Curve Cryptosystem.

UNIT – IV:

Message Integrity and Message Authentication: Message Authentication Code (MAC), SHA-512 - Digital Signatures.

UNIT – V:

Security at the Application Layer: PGP and S/MIME. Security at Transport Layer: SSL and TLS. -Principles of IDS, Virus, Firewalls, Virus Counter measures – Firewall Design Principles – Trusted Systems.

TEXT BOOKS:

1. Computer Networks, Andrew S Tanenbaum, David. J. Wetherall, 5th Edition, Pearson Education/PHI
2. Cryptography & Network Security, Behrouz A. Forouzan, Special Indian Edition, Tata McGraw-Hill

REFERENCES:

1. Network Security Essentials (Applications and Standards), William Stallings, Pearson Education
2. Cryptography and Network Security – Principles and Practices, William Stallings, 4th Edition, Prentice Hall of India, 2005
3. Security in Computing, Charles B. Pfleeger, Shari Lawrence Pfleeger, 3rd Edition, Pearson Education, 2003

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) V Semester

(22MC2CY301) PRINCIPLES OF INFORMATION SECURITY LABORATORY

TEACHING SCHEME		
L	T/P	C
0	3	1.5

EVALUATION SCHEME					
D-D	PE	LR	CP	SEE	TOTAL
10	10	10	10	60	100

COURSE OBJECTIVES:

- To apply algorithms used for data encryption and decryption
- To demonstrate IDS tools
- To apply algorithms used for message Integrity and authentication of data
- To understand various protocols for information security to protect against the threats in the networks

COURSE OUTCOMES: After completion of course, the students should be able to

CO-1: Implement various encryption and decryption algorithms
CO-2: Identify the emerging areas in information security
CO-3: Interpret good security practices for information security
CO-4: Demonstrate the process of data protection from various threats

LIST OF EXPERIMENTS:

1. Write a program to perform encryption and decryption using the following substitution ciphers.
    a. Caeser cipher
    b. Play fair cipher
    c. Hill Cipher
2. Write a program to implement the DES algorithm.
3. Write a program to implement RSA algorithm.
4. Calculate the message digest of a text using the SHA-1 algorithm.
5. Working with sniffers for monitoring network communication (Wireshark).
6. Configuring S/MIME for email communication.
7. Using Snort, perform real time traffic analysis and packet logging.

TEXT BOOKS:

1. Cryptography and Network Security, William Stallings, 3rd Edition, Pearson Education
2. Applied Cryptography, Bruce Schneier, John Wiley, 1996

REFERENCES:

1. Cryptography and Network Security, Behrouz A. Forouzan, McGraw-Hill, 2008
2. Security in Computing, Charles B. Pfleeger, Shari Lawrence Pfleeger, 3rd Edition, Pearson Education,2003

VNR VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

B.Tech. Minor (CYS) VI Semester

(22MC1CY302) FOUNDATIONS of CYBER SECURITY

TEACHING SCHEME		
L	T/P	C
3	1	4

EVALUATION SCHEME				
SE	CA	ELA	SEE	TOTAL
30	5	5	60	100

COURSE OBJECTIVES:

- To summarize various types of cyber-attacks and cyber-crimes
- To understand cyber laws and the concepts of digital forensics
- To discuss safety measures for the protection of mobile and wireless devices
- To learn the organizational security implications and threats
- To study the impact of data privacy attacks on various domains

COURSE OUTCOMES: After completion of the course, the student should be able to

CO-1: Identify the need of cyber security and various types of attacks

CO-2: Understand national and international regulations of cyber security and cyber forensics

CO-3: Interpret the security challenges related to mobile and wireless devices

CO-4: Analyze the security and privacy implications of an organization

CO-5: Examine the data privacy concepts and cybercrime in different domains

UNIT – I:

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT – II:

Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics

UNIT – III:

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

UNIT – IV:

Cyber Security: Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations

UNIT – V:

Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc. Cybercrime: Examples and Mini-Cases Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:

1. Cyber Security Understanding Cyber Crimes, Nina Godbole and Sunit Belpure, Computer Forensics and Legal Perspectives, Wiley
2. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, B. B. Gupta, D. P. Agrawal, Haoxiang Wang, CRC Press, 2018

REFERENCES:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press
2. Introduction to Cyber Security, Chwan-Hwa (John) Wu, J. David Irwin, CRC Press, T&F Group