Scheme of Instruction & Examination
B. E. – MINOR –Cybersecurity
V SEMESTER

S. No.	Course Code	Course Title	Scheme of Instruction				Scheme of Examination		Credits
			L	T	P / D	Contact Hours / week	CIE	SEE	
Theory Courses									
1	CYS-01CS	Cryptography and Network Security	3	0	0	3	40	60	3
2	CYS-02CS	Foundations of Cyber Security	3	0	0	3	40	60	3
Practical / Laboratory Courses									
3	CYS-03CS	Cryptography and Network Security Lab	0	0	2	2	40	60	1
		Total Credits				**08**	**120**	**180**	**07**

VI SEMESTER

S. No.	Course Code	Course Title	Scheme of Instruction				Scheme of Examination		Credits
			L	T	P / D	Contact Hours / week	CIE	SEE	
Theory Courses									
1	CYS-04CS	Ethical Hacking	3	0	0	3	40	60	3
Practical / Laboratory Courses									
2	CYS-05CS	CISCO Cyber Security Lab(Self Learning Course)						60	1
		Total Credits				**03**	**40**	**120**	**04**

VII SEMESTER

S. No.	Course Code	Course Title	Scheme of Instruction				Scheme of Examination		Credits
			L	T	P / D	Contact Hours / week	CIE	SEE	
Theory Courses									
1	CYS-06CS	Cyber Crime Investigation and Digital Forensics	3	0	0	3	40	60	3
Practical / Laboratory Courses									
2	CYS-07CS	Project Work	0	0	4	4	40	60	4
		Total Credits				**07**	**80**	**120**	**07**

V SEMESTER

Course Code	Course Title						Core / Elective
CYS-01CS	**CRYPTOGRAPHY AND NETWORK SECURITY**						**PE-1**
Prerequisite	**Contact Hours per Week**				**CIE**	**SEE**	**Credits**
	L	**T**	**D**	**P**			
ATD	**3**	**-**	**-**	**-**	**40**	**60**	**3**

COURSE OBJECTIVES:

The objective of this course is to make the student to

1. Explain the importance and application of each of confidentiality, integrity, authentication and availability
2. Understand various cryptographic algorithms.
3. Understand the basic categories of threats to computers and networks
4. Describe public-key cryptosystem.
5. Describe the enhancements made to IPv4 by IPSec
6. Understand Intrusions and intrusion detection and Discuss the fundamental ideas of public-key cryptography

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

1. Understand basic cryptographic algorithms, message and web authentication and security issues.
2. Distinguish Secure message transfer over insecure channel transfer.
3. Summarize the Confidentiality, Integrity and Availability of a data.
4. Explain various public and private key cryptography algorithms.
5. Apply digital signature to an application

UNITI

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks..

UNITII

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

UNITIII

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures. Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Public – Key Infrastructure

UNITIV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH)
Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security

UNITV

E-Mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange
Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

TEXT BOOKS

1. Cryptography and Network Security – Principles and Practice: William Stallings, VI Edition ,Pearson Education
2. Cryptography and Network Security: AtulKahate, III Edition, Mc Graw Hill

REFERENCE BOOKS

1. Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, II Edition, CRC Press, 2015.
2. Introduction to Cryptography, Johannes A. Buchmann, II Edition, Springer-Verlag, 2003.

Course Code	Course Title						Core / Elective
CYS-02CS	**FOUNDATIONS OF CYBER SECURITY**						**PE-1**
Prerequisite	**Contact Hours per Week**				**CIE**	**SEE**	**Credits**
	L	**T**	**D**	**P**			
ATD	**3**	**-**	**-**	**-**	**40**	**60**	**3**

COURSE OBJECTIVES:

1. The objective of this course is to make the student to
2. To understand various types of cyber-attacks and cyber-crimes
3. To learn threats and risks within context of the cyber security
4. To have an overview of the cyber laws & concepts of cyber forensics
5. To study the defensive techniques against these attacks

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

1. Analyze and evaluate the cyber security needs of an organization.
2. Understand Cyber Security Regulations and Roles of International Law.
3. Design and develop a security architecture for an organization.
4. Understand fundamental concepts of data privacy attacks
5. 5.Analyze cybercrime frauds and cases in the society.

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.Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need forComputer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, DigitalForensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics

UNIT III

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and WirelessDevices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security

Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication serviceSecurity, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in MobileComputing Era, Laptops.

UNIT IV

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

UNIT V

Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Datalinking and profiling, privacy policies and their specifications, privacy policy languages,

privacy indifferent domains- medical, financial, etcCybercrime: Examples and Mini-CasesExamples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions ofRupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. MiniCases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, FinancialFrauds in Cyber Domain.

TEXT BOOKS

1. Cyber Security Understanding Cyber Crimes, ComputerForensics and Legal Perspectives, Nina Godbole and SunitBelpure, Wiley.
2. Haoxiang Wang, Computer and Cyber Security: Principles,Algorithm, Applications, and Perspectives, B.B. Gupta, D.P. Agrawal,CRC Press, ISBN 9780815371335,2018.

REFERENCE BOOKS

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

Course Code	Course Title						Core / Elective
CYS-03CS	**CRYPTOGRAPHY AND NETWORK SECURITY LAB**						**PE-1**
Prerequisite	**Contact Hours per Week**				**CIE**	**SEE**	**Credits**
	L	**T**	**D**	**P**			
ATD	**-**	**-**	**-**	2	**40**	**60**	**1**

COURSE OBJECTIVES:

1. Explain the importance and application of each of confidentiality, integrity, authentication and availability
2. Understand various cryptographic algorithms.
3. Understand the basic categories of threats to computers and networks
4. Describe public-key cryptosystem.
5. Describe the enhancements made to IPv4 by IPSec
6. Understand Intrusions and intrusion detection and Discuss the fundamental ideas of public-key cryptography.

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

1. Understand basic cryptographic algorithms, message and web authentication and security issues.
2. Distinguish Secure message transfer over insecure channel transfer.
3. Summarize the Confidentiality, Integrity and Availability of a data.
4. Explain various public and private key cryptography algorithms.
5. Apply digital signature to an application.

1.Program that contains a string(char pointer) with a value \HelloWorld'.Theprograms should XOR each character in this string with 0 anddisplay the result.
2. Program that contains a string (char pointer) with a value \HelloWorld'. The program should AND or and XOR each character in this stringwith 127 and display the result.
3. Program to perform encryption anddecryption using the following algorithms:
   a. Ceaser Cipher
   b. Substitution Cipher
   c. Hill Cipher
4. Program to implement the DES algorithm logic
5. Program to implement the Blowfish algorithm logic
6. Program to implement RSA Algorithm
7. Program to implement Diffie Hellman Key Exchange
8. Program to calculate message digest of a text using MD5 /SHA -1 algorithm

VI SEMESTER

Course Code	Course Title						Core / Elective
CYS-04CS	**ETHICAL HACKING**						**PE-1**
Prerequisite	**Contact Hours per Week**				**CIE**	**SEE**	**Credits**
	L	**T**	**D**	**P**			
ATD	**3**	**-**	**-**	**-**	**40**	**60**	**3**

COURSE OBJECTIVES:

1. Understand the basics of computer based vulnerabilities.
2. Explore different foot printing, reconnaissance and scanning methods.
3. Expose the enumeration and vulnerability analysis methods.
4. Understand hacking options available in Web and wireless applications.
5. Explore the options for network protection.

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

1. Understand the basics of computer based vulnerabilities
2. Understand the different foot printing, reconnaissance and scanning methods.
3. Demonstrate the enumeration and vulnerability analysis methods
4. Acquire knowledge on the options for network protection.
5. Use tools to perform ethical hacking to expose the vulnerabilities.

UNITI

Ethical Hacking Overview - Role of Security and Penetration Testers- Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer - The Internet Layer - IP Addressing- Network and Computer Attacks - Malware - Protecting Against Malware Attacks- Intruder Attacks - Addressing Physical Security.

UNIT II

Foot printing, Reconnaissance and ScanningNetworks:Footprinting Concepts - Footprinting through Search Engines, Web Services, Social Networking Sites, Website, Email - Competitive Intelligence – Footprinting through Social Engineering - Footprinting Tools - Network Scanning Concepts - Port-Scanning Tools - Scanning Techniques - Scanning Beyond IDS and Firewall

UNIT III

Enumeration and Vulnerability Analysis: Enumeration Concepts - NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration - Vulnerability Assessment Concepts - Desktop and Server OS Vulnerabilities - Windows OS Vulnerabilities - Tools for Identifying Vulnerabilities in Windows- Linux OS Vulnerabilities- Vulnerabilities of Embedded Oss

UNIT IV

System Hacking: Hacking Web Servers - Web Application Components- Vulnerabilities - Tools for Web Attackers and Security Testers Hacking Wireless Networks - Components of a Wireless Network – WardrivingWireless Hacking - Tools of the Trade

UNIT V

Network Protection System: Access Control Lists. - Cisco Adaptive Security Appliance Firewall - Configuration and Risk Analysis Tools for Firewalls and Routers - Intrusion Detection and Prevention Systems - Network-Based and Host-Based IDSs and IPSs - Web Filtering - Security Incident Response Teams – Honeypots

TEXT BOOKS

1. Hands-On Ethical Hacking andNetwork Defense, Course Technology, Michael T. Simpson, Kent Backman, and James E. Corley, Delmar Cengage Learning, 2010.
2. The Basics of Hacking and Penetration Testing - Patrick Engebretson, SYNGRESS, Elsevier, 2013.

REFERENCE BOOKS

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, DafyddStuttard and Marcus Pinto, 2011.
2. The Ethical Hacker's Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams Grey Hat Hacking,III Edition, 2011, The McGraw-HillCompanies.

CISCO CYBERSECURITY LAB[SELF LEARNING]

Semester VI	**L**	**T**	**P**	**Credits**
Subject code –CYS-05CS	**0**	**0**	**0**	**1**

MODULE 1 : Introduction to Cybersecurity

Syllabus:

1. Need for Cybersecurity
2. Attacks, concepts and techniques
3. Protecting your data and privacy
4. Protecting the organization
5. Will your future be cybersecurity

MODULE 2 : Cybersecurity Essentials

VII SEMESTER

Course Code	Course Title						Core / Elective
CYS-06CS	**CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS**						**PE-1**
Prerequisite	**Contact Hours per Week**				**CIE**	**SEE**	**Credits**
	L	**T**	**D**	**P**			
ATD	**3**	**-**	**-**	**-**	**40**	**60**	**3**

COURSE OBJECTIVES:

1. To understand various types of cyber-attacks and cyber-crimes
2. To learn investigation tools
3. To have an overview forensic technology
4. To study laws, ethics and handling procedures
5. To learn Acts and legal policies

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

1. Understand the fundamentals of cybercrime and issues.
2. Understand different investigation tools for cybercrime.
3. Understand basics of Forensic technology and Practices.
4. Analyze different laws, ethics and evidence handling procedures.
5. Analyze the Acts and legal policies..

UNIT I

Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types ofCyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT II

Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes,Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, SoftwarePiracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital lawsand legislation, Law Enforcement Roles and Responses.

UNIT III

Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, DigitalEvidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-MailRecovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure ofComputers, Recovering Deleted Evidences, Password Cracking.

UNIT IV

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis andAdvanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Irisand Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux SystemForensics, Network Forensics.

UNIT V

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basicsof Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.

TEXT BOOKS

1. Computer Forensics and Investigations,Nelson Phillips and EnfingerSteuart, CengageLearning, New Delhi, 2009.
2.Incident Response and Computer Forensics,Kevin Mandia, Chris Prosise, Matt Pepe, TataMcGraw -Hill, New Delhi, 2006.

REFERENCE BOOKS

1. Software Forensics, Robert M Slade, Tata McGraw - Hill, New Delhi, 2005.
2. Cybercrime, Bernadette H Schell, Clemens Martin, ABC – CLIO Inc, California, 2004.
3. Understanding Forensics in IT , NIIT Ltd, 2005.

PROJECT WORK

Semester VII	L	T	P	Credits
Subject code: CYS-07CS	**0**	**0**	**4**	**4**

The Viva-Voce shall be conducted by a committee consisting of HOD, Project Supervisor and an External Examiner nominated by the University. The Internal Evaluation shall be made by the departmental committee, on the basis of two seminars given by each student on the topic of his/her project.

Project Proposal:

- Begin by developing a clear and well-defined project proposal. This should include a project title, objectives, scope, and a brief overview of the problem or area of interest.
- Specify the technologies, tools, and programming languages that will be used in the project.

2. Project Advisor:

- Assign a faculty member as a project advisor to guide and mentor the student throughout the project.

3. Project Selection:

- Choose a project that aligns with the program's objectives and your own interests. The project should be challenging and relevant to the field of computer science and engineering.
- Consider projects that involve software development, algorithm design, database management, data analysis, or other relevant areas.

4. Research and Literature Review:

- Conduct a thorough literature review to understand existing solutions and research related to your project.
- Identify gaps in the current knowledge and explain how your project will contribute to addressing these gaps.

5. Implementation:

- Begin the implementation phase by writing code, developing algorithms, or creating software as per your project's requirements.

- Ensure that your code adheres to coding standards and best practices.

6. Testing and Debugging:

- Rigorously test your project to identify and resolve bugs and errors.

- Perform unit testing, integration testing, and user acceptance testing as applicable.

7. Documentation:

- Maintain comprehensive documentation throughout the project. This includes code comments, user manuals, design documents, and technical reports.
- Properly cite and reference any external sources or libraries used in your project.

8. Presentation and Demo:

- Prepare a well-structured presentation and a live demonstration of your project's functionality.
- Highlight the problem statement, methodology, key features, and the impact of your project.

11. Final Report: - Submit a comprehensive final report that summarizes your project from start to finish. Include all documentation, code, and research findings.

12. Presentation: - Be prepared to present and defend your project in front of panel.

13. Future Work and Impact: - Discuss potential future work or enhancements that could be made to your project.