Pandit Deendayal Energy University,
Gandhinagar

School of Technology

Computer Science and Engineering

Post Graduate Curriculum Handbook

M.Tech.

(Cyber Security)

Program Educational Objectives (PEOs)

PEO-1 Graduate will be successfully recognized as superiors for their problem solving capabilities and professional skills in the field of Cyber Security.

PEO-2 Graduate pursue higher studies or research career by acquiring in depth knowledge in cyber security and allied fields.

Program Outcomes (POs)

PO-1 An ability to independently carry out research /investigation and development work to solve practical problems.

PO-2 An ability to write and present a substantial technical report/document.

PO-3 Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.

PO-4 Design and Innovate computing systems addressing diverse needs in the domain of cyber security.

PO-5 Analyze the requirements of cyber security and design operational strategies and policies.

PO-6 Use cyber security solutions to analyze ethical, legal and social implications to solve real world problems.

Ist Semester

PANDIT DEENDAYAL ENERGY UNIVERSITY GANDHINAGAR

SCHOOL OF TECHNOLOGY

COURSE STRUCTURE FOR M.TECH - CYBER SECURITY

Semester I			**M. Tech. - Cyber Security**										
Sr. No	**Course Code**	**Course Name**	**Teaching Scheme**					**Exam Scheme**					**Total**
								Theory			**Practical**		
			L	**T**	**P**	**C**	**Hrs /wk**	**MS**	**ES**	**IA**	**LW**	**LE/ Viva**	**Marks**
1	20MA502T	Mathematical Foundation of Cyber Security	3	1	0	4	4	25	50	25	--	--	100
2	20CS501T	Algorithms and Complexity	3	0	0	3	3	25	50	25	--	--	100
3	20CS501P	Algorithms and Complexity Lab	0	0	2	1	2	--	--	--	50	50	100
4	20CS502T	Cryptography and Network Security	3	0	0	3	3	25	50	25	--	--	100
5	20CS502P	Cryptography and Network Security Lab	0	0	2	1	2	--	--	--	50	50	100
6	20CS503T	Cyber Forensics	3	0	0	3	3	25	50	25	--	--	100
7	20CS503P	Cyber Forensics Lab	0	0	2	1	2	--	--	--	50	50	100
8	20CS504P	Cyber Security Tools I	0	0	4	2	4	0	0	0	50	50	100
9	20CS505P	Capstone Project I	0	0	4	2	4	0	0	0	50	50	100
		Total	**12**	**1**	**14**	**20**	**27**	**100**	**200**	**100**	**200**	**200**	**900**

MS = Mid Semester, ES = End Semester; IA = Internal assessment (like Test/quizzes, assignments etc.)

LW = Laboratory work; LE = Laboratory Exam

20MA502T					Mathematical Foundation of Cyber Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	1	0	4	4	25	50	25	--	--	100

COURSE OBJECTIVES

- To provide fundamental concept of abstract algebra.
- To study basic concepts of set theory and binary operations.
- To study different operations on algebraic structure.
- To study advanced number theory concepts.

UNIT 1 GROUP THEORY **13 Hrs.**

Introduction to Set Theory, Binary Operations on Sets, Matrix and Vector Algebra, Equivalence Relations, Introduction to Groups, Subgroups, Cyclic Groups, dihedral groups , Permutation Groups, Caley theorem, cosets, Lagrange's theorem, Normal Subgroups, Quotient Groups, Isomorphisms, Homomorphisms.

UNIT 2 RINGS **13 Hrs.**

Definition and basic concepts in rings, examples and basic properties, zero divisors, integral domains, fields, characteristic of a ring, quotient field of an integral domain, subrings, ideals, maximal ideal, prime ideal, quotient rings, isomorphism theorems. Euclidean domains, commutative rings, Divisibility, Primes, GCDs, and the Euclidean Algorithm, Congruence.

UNIT 3 FIELDS **13 Hrs.**

Ring of polynomials, prime, irreducible elements and their properties. Eisensteins irreducibility criterion and Gauss's lemma. UFD, PID and Euclidean domains. Ring of polynomials over a field, field extensions, algebraic and transcendental elements, algebraic extensions, splitting field of a polynomial, algebraic closure of a field, Integral domains and fields, polynomial representation of binary number, Finite fields, Fundamental Theorem of Galois Theory.

UNIT 4 ADVANCED NUMBER THEORY **13 Hrs.**

Advanced Number Theory – Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence, Discrete Logarithm, Factorization Methods, Side Channel Attacks, Shannon Theory, Perfect Secrecy, Semantic Security.

Max. 52 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Define the concepts related to the basics of set theory and binary operations.
CO2- Demonstrate knowledge and understanding of groups, subgroups, and order of an element in finite groups.
CO3- Develop understanding of algebraic structure ring, and field.
CO4- Discover different operations on algebraic structure.
CO5- Choose appropriate algebraic structure for cryptographic operation.
CO6- Develop understanding of use of algebraic structure in number theory algorithms.

TEXT/REFERENCE BOOKS

1. D.S. Dummit and R.M. Foote, "Abstract Algebra", John Wiley
2. Michael Artin, "Algebra", Pearson Education.
3. J.A. Gallian, "Contemporary Abstract Algebra", Narosa Publishing House.
4. I. N. Herstein, "Topics in Algebra", Wiley.
5. N. Jacobson, "Basic Algebra I", Hindustan Publishing Company.
6. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS501T					Algorithms and Complexity					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- Analyze the asymptotic performance of the algorithms
- To review data structure topics.
- To review algorithm techniques.
- To study and apply hash functions in real time.

UNIT 1 INTRODUCTION 10 Hrs.

Review of the Algorithmic - Terminologies - Computability Theory, Computational Complexity - average & worst-case analysis, Recurrences and Mathematical Background. Probability theory.

UNIT 2 ALGORITHM DESIGN TECHNIQUES AND ANALYSIS 10 Hrs.

Algorithmic paradigms: Divide-and-Conquer, Dynamic Programming, Greedy, Backtracking,Branch -and-bound; Amortized analysis.

UNIT 3 ADVANCED ALGORITHMS 10 Hrs.

Shortest paths, Minimum Spanning Trees - Flow networks - Bipartite Matching - Applications. Introduction to Approximation algorithms; Randomized algorithms.

UNIT 4 COMPLEXITY THEORY 09 Hrs.

NP-completeness - Complexity Classes. NP and co-NP, Reductions; Results on structure of NP - complete sets, Sparse NP-hard sets, Basic Inclusions and Separations, Nondeterministic Space Classes, Logarithmic Space, A PSPACE complete problem, Polynomial Hierarchy.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1-.Understand the algorithms for solving practical problems efficiently.
CO2- Define running times of algorithms using asymptotic analysis
CO3- Apply greedy algorithm technique to solve optimization problems.
CO4- Compare algorithms in terms of time complexity, and space utilization.
CO5- Determine complexity analysis of computational, optimization and graph problems.
CO6- Design algorithms for computational problems of moderate complexity.

TEXT/REFERENCE BOOKS

1. T.H. Cormen, C.E. Leiserson, R.L. Rivest, Stein; “Introduction to Algorithms”, MIT Press, USA.
2. P. Raghavan and R. Motwani., “Randomized Algorithms”; Cambridge University Press, UK.
3. M.T. Goodrich, R. Tamassia, M.H. Goldwasser; “Data Structures and Algorithms in Python”. John Wiley & Sons, USA.
4. D.L. Ranum and B.N. Miller; “Problem Solving with Algorithms and Data Structures using Python”, Franklin, Beedle and Associates Inc., USA

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS501P					Algorithms and Complexity Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
-	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- Analyse the asymptotic performance of the algorithms
- To review data structure topics.
- To review algorithm techniques.
- To study and apply hash functions in real time.

LIST OF EXPERIMENT

Experiment Sessions using Programming would be based on following topics:
Basics of data structure, dynamic programming, algorithm analysis, divide and conquer.
Following list gives some programming examples. Faculty can prepare their own list in same manner keeping guidelines and subject syllabus in mind.

1. Write a program for recursive and no recursive Fibonacci sequence with affecting factors
2. Write a program for merge sort and do the analysis
3. Write a program for merge sort and do the analysis
4. Write a program for quick sort and do the analysis
5. Program to explore the divide and conquer programming like Exponentiation, Binary Search, strassen's matrix multiplication.
6. Program to explore the greedy programming like Job Scheduling, Single Source Shortest Path, Huffman Coding, Fractional Knapsack, Activity Selection.
7. Program to explore the dynamic programming 0-1 Knapsack, All Pair Shortest Path, Making Change.
8. Use of NP theory complexity in cyber security topics.

COURSE OUTCOMES

On completion of the course, student will be able to
CO1-.Understand the algorithms for solving practical problems efficiently.
CO2- Define running times of algorithms using asymptotic analysis
CO3- Apply greedy algorithm technique to solve optimization problems.
CO4- Compare algorithms in terms of time complexity, and space utilization.
CO5- Determine complexity analysis of computational, optimization and graph problems.
CO6- Design algorithms for computational problems of moderate complexity.

TEXT/REFERENCE BOOKS

1. T.H. Cormen, C.E. Leiserson, R.L. Rivest, Stein; “Introduction to Algorithms”, MIT Press, USA.
2. P. Raghavan and R. Motwani., “Randomized Algorithms”; Cambridge University Press, UK.
3. M.T. Goodrich, R. Tamassia, M.H. Goldwasser; “Data Structures and Algorithms in Python”. John Wiley & Sons, USA.
4. D.L. Ranum and B.N. Miller; “Problem Solving with Algorithms and Data Structures using Python”, Franklin, Beedle and Associates Inc., USA

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS502T					Cryptography and Network Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study use of cryptography.
- To study cryptographic algorithms.
- To study identification of cryptosystem.
- To study concept of network security.

UNIT 1 INTRODUCTION **10 Hrs.**

Introduction : Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model, CIA model, Introduction to Classical Cryptography, Cryptanalysis of Cryptosystems.

UNIT 2 BLOCK CIPHERS **08 Hrs.**

Introduction to symmetric key cryptography, Feistal Cipher Structure, DES, AES, Security analysis of Symmetric key algorithms, Block Cipher design principles, Pseudo Random Number Generation.

UNIT 3 PUBLICK KEY CRYPTOGRAPHY AND HASH FUCNTION **12 Hrs.**

Principles Of Public-Key Cryptography, Diffie- Hellman Key Exchange, The RSA Cryptosystems; Semantic Security of RSA, Hash Function, Digital Signature.

UNIT 4 INTRODUCTION TO NETWORK SECURITY **09 Hrs.**

Security at Application Layer – Email, PGP, S/MIME, Security at Transport Layer – SSL, TLS, HTTPs, Security at Network Layer – IPSec, Wireless Network Security – IEEE 802.11.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Define the Symmetric and Asymmetric Cryptographic Techniques.
CO2- Understand CIA Model
CO3- Implement the public key cryptographic techniques for securing the data in transit.
CO4- Compare the Security strength of cryptography techniques.
CO5- Apply hashing techniques and digital signatures for integrity and authentication.
CO6- Analyze the network security with network security tools.

TEXT/REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.
2. AtulKahate, “Cryptography and Network Security”, Tata McGraw-Hill Education.
3. Menezes, Oorschot, Vanstone : "Handbook of Applied Cryptography", CRC Press
4. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
5. Douglas Stinson, “Cryptography: Theory and Practice”, Taylor & Francis.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS502P					Cryptography and Network SecurityLab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study use of cryptography.
- To study cryptographic algorithms.
- To study identification cryptosystem.
- To study concept of digital signature.

LIST OF EXPERIMENT

Experiment Sessions using Programming would be based on following topics:

Basics of classical ciphers, cryptographic algorithms, hash function, identification schemes.

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Write a program to break a ciphertext generated using affine cipher by brute-force approach.
2. Write a program to implement extended Euclidean algorithm.
3. Implement modular exponentiation algorithm
4. Write a program to implement CCA-2 attack on RSA.
5. Explain with implementation, how a small sub-group can affect the security of Diffie-Hellman Key exchange.
6. Implement SHA-256 algorithm
7. Download and practice Wireshark tool
8. Study and implement information security related latest research papers.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Define the Symmetric and Asymmetric Cryptographic Techniques.
CO2- Understand CIA Model
CO3- Implement the public key cryptographic techniques for securing the data in transit.
CO4- Compare the Security strength of cryptography techniques.
CO5- Apply hashing techniques and digital signatures for integrity and authentication.
CO6- Analyze the network security with network security tools.

TEXT/REFERENCE BOOKS

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.
2. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Wiley Computer Publishing.
3. AtulKahate, “Cryptography and Network Security”, Tata McGraw-Hill Education.
4. Menezes, Oorschot, Vanstone : "Handbook of Applied Cryptography", CRC Press
5. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
6. Douglas Stinson, “Cryptography: Theory and Practice”, Taylor & Francis.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS503T					Cyber Forensics					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study the technical perspective of cyber forensics.
- To study the forensic science and code of ethics.
- To study various operating system platforms.
- To study anti forensic tools.

UNIT 1 INTRODUCTION TO CYBERCRIME **10 Hrs.**

Cybercrimes- The Technical perspective, abuse & misuse of technologies; Introduction to Cybercrime laws of India - Understanding of the overall Investigative process.

UNIT 2 DIGITAL FORENSIC **10 Hrs.**

Locard's principle, Basics of digital forensics. Different storage media, Code of ethics in Digital forensics investigation; Introduction to Proprietary & Open source investigation tools.

UNIT 3 ASSESSMENT OF DIGITAL EVIDENCE **10 Hrs.**

Assessment of Digital evidence. Mobile device forensics. Storage locations, Different platforms. Acquisition of Digital evidence. Examination of Digital evidence. Documentation and reporting.

UNIT 4 CYBER FORENSICS **09 Hrs.**

Cloud forensics. Anti-forensics tools. Data Destruction programs. SWGDE model.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand cyber forensics.
CO2- Demonstrate an understanding of issues related to privacy and determine how to address them technically and ethically.
CO3- Apply digital forensics analysis upon different platforms.
CO4- Measures the method of cybercrimes.
CO5- Determine cyber forensic process.
CO6- Design policies and procedures for incident response.

TEXT/REFERENCE BOOKS

1. Eoghan Casey, "Handbook of Computer Crime Investigation Forensic Tools and Technology", Academic Press.
2. John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics", Syngress Media.
3. Harlan Carvey, "Windows Forensics and Incident Recovery", Addison-Wesley Professional.
4. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS503P					Cyber Forensics Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study the technical perspective of cyber forensics.
- To study the forensic science and code of ethics.
- To study various operating system platforms.
- To study anti forensic tools.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Study and Practice cyber forensics tools.
2. Perform cyber forensics analysis on different storage media with different platform like android operating system, windows operating system, etc.
3. Practice acquisition of digital evidence with different environment and different techniques.
4. Perform examination of digital evidence like email investigation, registry forensics, etc.
5. Study and Practice Anti Forensics tools.
6. Setting up a Cyber Forensics laboratory as part of the Incident response team - Policies & procedures; Quality assurance; Tools & equipment's; Accreditation;

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand cyber forensics.
CO2- Demonstrate an understanding of issues related to privacy and determine how to address them technically and ethically.
CO3- Apply digital forensics analysis upon different platforms.
CO4- Measures the method of cybercrimes.
CO5- Determine cyber forensic process.
CO6- Design policies and procedures for incident response.

TEXT/REFERENCE BOOKS

1. Eoghan Casey, "Handbook of Computer Crime Investigation Forensic Tools and Technology", Academic Press.
2. John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics", Syngress Media.
3. Harlan Carvey, "Windows Forensics and Incident Recovery", Addison-Wesley Professional.
4. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS504P					Cyber Security Tools – I					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	4	2	4	--	--	--	50	50	100

COURSE OBJECTIVES

- To install and understand cyber security tools
- To apply various languages in use of cyber security
- To study reverse engineering process
- To study penetration testing

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. VA-PT: Vulnerability Analysis, Penetration Testing.
2. Scripting languages: Common scripting language constructs, dynamic language features, client-side & server-side web scripting, Popular scripting languages, javascript, perl, php, python, ruby.
3. Penetration Testing : Penetration testing, methodologies, metrics, management, information gathering, vulnerability identification & verification, compromising a system & privilege escalation, maintaining access & covering the tracks.
4. Debugging: Reverse engineering, static & dynamic analysis, disassembly, debugging, setting up penetration lab, reporting results, cleaning up the lab, CTF assignment.

COURSE OUTCOMES

On completion of the course, student will be able to
CO1- Under Cyber Security Tools.
CO2- Classify offensive/defensive security tools on a working network.
CO3- Develop understanding of various client/server side scripting languages to build applications.
CO4- Compare vulnerabilities related to computer system and networks.
CO5- Evaluate best practices in security concepts to maintain security requirement of computer systems.
CO6- Choose cyber security tools for real time problems.

TEXT/REFERENCE BOOKS

1. Georgia Weidman, “Penetration Testing: A Hands-On Introduction to Hacking”, No Starch Press.
2. Peter Kim, “The Hacker Playbook 2: Practical Guide To Penetration Testing”, CreateSpace Independent Publishing Platform.
3. Patrick Engebretson; “The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy”, Syngress.
4. David Kennedy, Jim O'Gorman, Devon Kearns, MatiAharoni; “Metasploit: The Penetration Tester's Guide”, No Starch Press.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS505P					Capstone Project I					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	4	2	4	-	-	-	50	50	100

COURSE OBJECTIVES

- To enable students to define and design the precise cyber security based solution for a problem definition
- To encourage students to identify the various research challenges in the field of cyber security from the vast array of literature available
- To create awareness among the students of the characteristics of several domain areas where cyber security can be effectively used.
- To improve the team building, communication and management skills, presentation, and writing skills in societal and professional life.

SCOPE OF WORK:

The students are expected to work on Research Project in any of the Cyber Security related areas. The different kinds of projects and the associated deliverables that could be accepted as the student's Comprehensive Project are as follows but not limited to:

- Software Development,
- System Design and Simulation,
- Hardware Development/Implementation,
- Embedded System (Software & Hardware combined) Development / Implementation,
- Theoretical Modelling,
- Design and Analysis,
- Designing Advanced Algorithm/methods as a solution for the current cyber security challenges.
- Technical Study including feasibility and comprehensive evaluation of technologies,
- Technical Survey and Modelling,
- Modules of a research and development project.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 – Thoroughly study and analyze the problem definition.
CO2 - Think innovatively on the development of components, products, processes or technologies in the engineering field.
CO3 – Design and develop new concepts in multidisciplinary area.
CO4 - Apply the class-room learning to solve real world problems in the form of a team.
CO5 – Experiment with different tools and technologies to implement the solution.
CO6 - Prepare and present the technical reports/research papers.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on Presentation, Report and Viva	30 Marks
Part B: Evaluation Based on Presentation, Report and Viva	30 Marks
Part B: Evaluation Based on Presentation, Report and Viva	40 Marks

2nd Semester

PANDIT DEENDAYAL ENERGY UNIVERSITY GANDHINAGAR

SCHOOL OF TECHNOLOGY

COURSE STRUCTURE FOR M.TECH - CYBER SECURITY													
Semester II			**M. Tech. - Cyber Security**										
Sr. No	**Course Code**	**Course Name**	**Teaching Scheme**					**Exam Scheme**					**Total**
								Theory			**Practical**		
			L	**T**	**P**	**C**	**Hrs /wk**	**MS**	**ES**	**IA**	**LW**	**LE/ Viva**	**Marks**
1	20CS506T	Secure Programming	3	0	0	3	3	25	50	25	--	--	100
2	20CS506P	Secure Programming Lab	0	0	2	1	2	--	--	--	50	50	100
3	20CSXXXT	Department Elective I	3	0	0	3	3	25	50	25	--	--	100
4	20CSXXXP	Department Elective I Lab	0	0	2	1	2	--	--	--	50	50	100
5	20CSXXXT	Department Elective II	3	0	0	3	3	25	50	25	--	--	100
6	20CSXXXP	Department Elective II Lab	0	0	2	1	2	--	--	--	50	50	100
7	20CSXXXT	Department Elective III	3	0	0	3	3	25	50	25	--	--	100
8	20CSXXXP	Department Elective III Lab	0	0	2	1	2	--	--	--	50	50	100
9	20CS507P	Cyber Security Tools II	0	0	4	2	4	0	0	0	50	50	100
10	20CS508P	Capstone Project II	0	0	4	2	4	0	0	0	50	50	100
11	17CE527T	Successful research and Development Program	2	0	0	2	2						NP/PP
		Total	**14**	**0**	**16**	**22**	**30**	**100**	**200**	**100**	**250**	**250**	**1000**

MS = Mid Semester, ES = End Semester; IA = Internal assessment (like Test/quizzes, assignments etc.)

LW = Laboratory work; LE = Laboratory Exam

List of Department Electives (Sem II)

Course Code	**Course Name**	**Department Elective Group**
20CS509P	Cyber Crime and Investigation - LAB	Department Elective - I
20CS509T	Cyber Crime and Investigation	Department Elective - I
20CS511P	Authentication Protocols in Cyber Space - LAB	Department Elective - I
20CS511T	Authentication Protocols in Cyber Space	Department Elective - I
20CS510P	Advanced Computer Security - LAB	Department Elective - I
20CS510T	Advanced Computer Security	Department Elective - I
20CS513P	Privacy in Cyber Network - LAB	Department Elective - II
20CS513T	Privacy in Cyber Network	Department Elective - II
20CS515P	Machine Learning in Cyber Security - LAB	Department Elective – II
20CS515T	Machine Learning in Cyber Security	Department Elective – II
20CS514P	Software Quality Assurance - LAB	Department Elective - II
20CS514T	Software Quality Assurance	Department Elective – II
20CS512P	Cyber Attacks & Defence - LAB	Department Elective – III
20CS512T	Cyber Attacks & Defence	Department Elective – III
22CS501T	Introduction to Blockchain Technology	Department Elective – III
22CS501P	Introduction to Blockchain Technology LAB	Department Elective – III
23CS501T	Web Penetration Testing	Department Elective – III
23CS501P	Web Penetration Testing LAB	Department Elective – III

****All students are required to complete 6 weeks industrial internship after first year and before commencement of second year.

20CS506T					Secure Programming					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand use of secure programming.
- To study buffer overflow related techniques.
- To study web security in present world.

UNIT 1 INTRODUCTION TO SECURE PROGRAMMING **10 Hrs.**

Software Security Issues & Defensive programming, Handling Program Input and Output, Writing Safe Program Code, Interacting with the Operating System and Other Programs.

UNIT 2 OVERFLOW ATTACKS **10 Hrs.**

Overflow: Buffer, stack, heap, global data, defending against overflows. Exploiting buffer overflows. Understand shellcode, Compiler-time & run-time defences, sandboxing, CERT Secure coding standards.

UNIT 3 SOCIAL ENGINEERING **10 Hrs.**

Advanced Persistent Threat, Viruses Propagation, Social Engineering – SPAM E-Mail, Trojans, Zombie, Bots, Phishing, Spyware, Backdoors, Rootkits, and Countermeasures.

UNIT 4 WEB APPLICATION SECURITY **09 Hrs.**

Introducing Web Application Security, Web Application Security Risk, Risk Assessment of Typical E-Commerce Web Applications; Critical web application security threats.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the basics of secure programming.
CO2- Explain the fundamental principles and mechanisms of software security.
CO3- Develop secure software development practices.
CO4-Discover the causes of security vulnerabilities and develop solutions to overcome these vulnerabilities.
CO5- Compare and contrast programming languages for secure features.
CO6- Create secure codes for use in real time systems.

TEXT/REFERENCE BOOKS

1. M. Howard and D. Leblanc, “Writing Secure Code”, Microsoft Press, USA.
2. A. Bhargav and B.V. Kumar, “Secure Java: For Web Application Development”, CRC Press, USA.
3. Page Kicker, Robot Phil, “OWASP Top 10: The Top 10 Most Critical Web Application Security Threats By OWASP”, CreateSpace Independent Publishing Platform.
4. John Viega and Matt Messier, “Secure Programming Cookbook for C and C++”, O’Reilly Media, USA.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS506P					Secure Programming Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand use of secure programming.
- To study buffer overflow related techniques.
- To study web security in present world.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Implement code to demonstrate buffer overflow attack.
2. Implement code to demonstrate heap overflow attack.
3. Implement code to demonstrate global data overflow attack.
4. Practice writing shell code.
5. Understand spam email, rootkits, backdoor, virus propagation, and spyware.
6. Perform risk assessment of web application.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the basics of secure programming.
CO2- Explain the fundamental principles and mechanisms of software security.
CO3- Develop secure software development practices.
CO4-Discover the causes of security vulnerabilities and develop solutions to overcome these vulnerabilities.
CO5- Compare and contrast programming languages for secure features.
CO6- Create secure codes for use in real time systems.

TEXT/REFERENCE BOOKS

1. M. Howard and D. Leblanc, “Writing Secure Code”, Microsoft Press, USA.
2. A. Bhargav and B.V. Kumar, “Secure Java: For Web Application Development”, CRC Press, USA.
3. Page Kicker, Robot Phil, “OWASP Top 10: The Top 10 Most Critical Web Application Security Threats By OWASP”, CreateSpace Independent Publishing Platform.
4. John Viega and Matt Messier, “Secure Programming Cookbook for C and C++”, O’Reilly Media, USA.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS507P					Cyber Security Tools – II					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	4	2	4	00	00	00	50	50	100

COURSE OBJECTIVES

- To study virtual targets and its analysis.
- To understand volatility framework.
- Analysis of malware in various environments.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. **MALWARE ANALYSIS**: Malware Analysis and Reverse Engineering, Types of malware; Malware analysis goals & techniques. Malware analysis in -Windows, Linux environment; Static vs. dynamic analysis.
2. **Malware LAB**: PE file headers; Setting up a malware analysis lab with Physical targets; Virtual targets and controller.Analyzing Physical and Process Memory Dumps for Malware Artefacts.
3. **MALWARE ANALYSIS IN VIRTUAL ENVIRONMENT**: Automated malware analysis in Virtual environment & monitoring with process monitor/explorer; IDAPro&Ollydb tools; kernel debugging; anti-reverse engineering.
4. **DEBUGGING:** Malware analysis using "Volatility Framework"; Case scenarios with to-do assignments - Examining a Malicious File Specimen; List of Windows/Linux functions commonly encountered by malware analysts.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand use of cyber security tools.
CO2- Explain the use various malware analysis techniques.
CO3- Apply practical investigations with Virtual Machines, RAM dump and mobile devices.
CO4- Classify various security tools on a working network.
CO5- Evaluate best practices in security concepts to maintain security requirement of computer systems.
CO6- Design solution to examine network traffic in decoded text format.

TEXT/REFERENCE BOOKS

1. Cameron H. Malin and James M. Aquilina, "Malware Forensics: Investigating and Analysing Malicious Code", Syngress Media.
2. Michael Sikorski, "Practical Malware analysis: The Hands-On Guide to Dissecting Malicious Software", No Starch Press.
3. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard; "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", Wiley.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS508P					Capstone Project II					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	4	2	4	-	-	-	50	50	100

COURSE OBJECTIVES

- To enable students to define and design the precise cyber security based solution for a problem definition
- To encourage students to identify the various research challenges in the field of cyber security from the vast array of literature available
- To create awareness among the students of the characteristics of several domain areas where cyber security can be effectively used.
- To improve the team building, communication and management skills, presentation, and writing skills in societal and professional life.

SCOPE OF THE WORK:

The students are expected to work on Research Project in any of the Cyber Security related areas. The different kinds of projects and the associated deliverables that could be accepted as the student's Comprehensive Project are as follows but not limited to:

- Software Development,
- System Design and Simulation,
- Hardware Development/Implementation,
- Embedded System (Software & Hardware combined) Development / Implementation,
- Theoretical Modelling,
- Design and Analysis,
- Designing Advanced Algorithm/methods as a solution for the current cyber security challenges.
- Technical Study including feasibility and comprehensive evaluation of technologies,
- Technical Survey and Modelling,
- Modules of a research and development project.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 – Thoroughly study and analyze the problem definition.
CO2 - Think innovatively on the development of components, products, processes or technologies in the engineering field.
CO3 – Design and develop new concepts in multidisciplinary area.
CO4 - Apply the class-room learning to solve real world problems in the form of a team.
CO5 – Experiment with different tools and technologies to implement the solution.
CO6 - Prepare and present the technical reports/research papers.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on Presentation, Report and Viva	30 Marks
Part B: Evaluation Based on Presentation, Report and Viva	30 Marks
Part B: Evaluation Based on Presentation, Report and Viva	40 Marks

17CE527T					Successful Research and Development Program					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
2	0	0	2	2	25	50	25	00	00	100

COURSE OBJECTIVES

- To develop understanding of the basic framework of research process
- To develop an understanding of various research designs and techniques.
- To identify various sources of information for literature review and data collection.
- To develop an understanding of the ethical dimensions of conducting applied research
- Appreciate the components of scholarly writing and evaluate its quality

9 Hrs.

UNIT 1 RESEARCH ORGANIZATION

Objectives & Goals of a Research Organization, Components of a research organization, Sponsors & Funding Agencies:Funding Agencies − Types**,** Types of Interface with Funding & Sponsor Agencies**,** Call for Proposals & Opportunity Tracking**,** Types of Proposals & Grants**,** Contracting Vehicles & Arrangements**,** Deliverables, Interim & Final Reviews**,** Cost & Performance Audits**,** Contract Laws

UNIT 2 <Development of Proposal Writing> **9 Hrs.**

Proposals for Research Program Funding: Center& Consortia Proposals, Individual Principal Investigator Proposals, Continuation & Renewal Proposals, PrimeſSubcontractor Relationships & Contracting, Cost Accounting, Laws and Regulations. intellectual Property & Patent Laws**,** Writing a Successful Research Proposal: Technical Proposal, Management Proposal, Cost Proposal, Technology Proposal, Statement of Work & Deliverables, Case Studies

UNIT 3 <Development of Research Methodology> **9 Hrs.**

The Research Process – I: Steps in development of successful research program, Quality and Cost consideration, Laboratories and infrastructure setup, Staffing & Support Models, Peer−Review, Independent Verification & Validation, Internal & External Review processes

UNIT 4: ETHICS AND LAWS

Ethics & Regulatory Laws & Guidelines, CaseStudies.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Students should be able to identify the overall process of designing a research study from its inception

CO2 - Students should understand the characteristics of various kinds of research (quantitative and qualitative

CO3 - Students should apply the knowledge of a forward chronological, backward chronological and manual search methods in framing the literature review for a scholarly educational study.

CO4 - Students should be analyze with conducting scholarly educational study: a. The steps in the overall process. b. The types of databases often searched. c. The criteria for evaluating the quality of a study. d. The ways of organizing the material found. e. The different types of literature reviews

CO5 - Student can able to exercise on various Ethical issues in conducting research.

CO6 - Develop research designs and project proposals in achieving project deliverables in stipulated period of time and cost.

TEXT/REFERENCE BOOKS

1. CR Kothari, Research Methodology (Methods and Techniques) book by New age Publications 3rd edition
2. Ranjith Kumar, Research Methodology book by Sage Publications 3rd edition (Softcopy Available)
3. PrathapHaridoss, Nptel Lectures: Introduction to Research,Prof. Department of Metallurgical and Materials Engineering, Indian Institute of Technology, Madras

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A/Question1: <identifying overall research process> <> Marks
Part A/Question2: <relation between quantitative and qualitative> <> Marks
Part A/Question3: <literature review process> <> Marks
Part A/Question4: <hypothesizing and concept building> <> Marks
Part A/Question5: <Ethical issues in conducting research> <> Marks

Department Electives (Sem II)

20CS509T					Cyber Crime and Investigation					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study cybercrimes.
- To investigate by certified authorities in cybercrime.
- To study IT Act.
- To study cyberspace and its applicability in real word.

UNIT 1 INTRODUCTION TO CYBERCRIME **10 Hrs.**

Introduction to Cyber Crime. Need for Cyber Law, Controlling And Preventing Cybercrime**.** Information Technology ACT 2000; E-Governance: Legal Recognition of Electronic Records.

UNIT 2 REGULATION TO CYBERCRIMES **10 Hrs.**

Regulating Certifying Authorities: Recognition of Foreign Authorities, License to Issue Electronic Signature Certificates; Penalty and Compensation for Damaging to Computer System, Compensation for Failure to Protect Data.

UNIT 3 CYBER OFFENCE UNDER IT Act **10 Hrs.**

Tampering with Computer Source Documents; Interception & Monitoring of Electronic Communications; Punishment for Cyber Terrorism; Offenses.

UNIT 4 INTERNATIONL LAW AND JURISDICTION IN CYBERSPACE **09 Hrs.**

Personal Jurisdiction in Cyberspace; Freedom of Expression and privacy in Cyberspace. Governance of social media. Intellectual property protection; Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the legislation and regulations that impact technology.
CO2- Demonstrate an understanding of issues related to privacy.
CO3- Identify standards of professionalism an ethical behaviour for information security.
CO4- Compare digital forensics principals.
CO5- Determine the legal and technical aspects of a cybercrime investigation.
CO6- Create the application of computer forensic tools.

TEXT/REFERENCE BOOKS

1. Vakul Sharma, “Information Technology Law and Practice: Law & Emerging Technology Cyber Law”, Universal Law Publishing.
2. Justice Yatindra Singh, “Cyber Laws”, Universal Law Publishing Co, New Delhi
3. David S. Wall, “Cybercrime: The Transformation of Crime in the Information Age”, Wiley Computer.
4. AnirudhRastogi, “Cyber Law of Information Technology and Internet”, LexisNexis.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS509P					Cyber Crime and Investigation Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study cybercrimes.
- To investigate by certified authorities in cybercrime.
- To study IT Act.
- To study cyberspace and its applicability in real word.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Study Computer Assisted Crime: virtual robberies, scams and thefts**.**
2. Study legal recognition of electronic records, legal recognition of electronic signatures, and publication of rule regulation in electronic gazette.
3. Study security procedures and practice, constitutional & human rights issues in cyberspace freedom of speech and expression in cyberspace, right to privacy, right to data protection.
4. Studyintellectual property protection; net neutrality, and other emerging issues such as data localization, cybercrimes & legal framework cybercrimes against individuals, institution and state.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the legislation and regulations that impact technology.
CO2- Demonstrate an understanding of issues related to privacy.
CO3- Identify standards of professionalism an ethical behaviour for information security.
CO4- Compare digital forensics principals.
CO5- Determine the legal and technical aspects of a cybercrime investigation.
CO6- Create the application of computer forensic tools.

TEXT/REFERENCE BOOKS

1. Vakul Sharma, “Information Technology Law and Practice: Law & Emerging Technology Cyber Law”, Universal Law Publishing.
2. Justice Yatindra Singh, “Cyber Laws”, Universal Law Publishing Co, New Delhi
3. David S. Wall, “Cybercrime: The Transformation of Crime in the Information Age”, Wiley Computer.
4. AnirudhRastogi, “Cyber Law of Information Technology and Internet”, LexisNexis.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS510T					Advanced Computer Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study principals in computer security.
- To study operating system security.
- To study database security.

UNIT 1 INTRODUCTION TO ADVANCED PUBLIC KEY CRYTPOGRAPHY **10 Hrs.**

Goldwasser-Micali Cryptosystem; Paillier Cryptosystem; Elliptic Curve Arithmetic, Elliptic Curve Cryptography, Pseudorandom Number Generation, Identity Based Cryptography, Attribute Based Cryptography, Multi Party Protocols – Secret Sharing.

UNIT 2 INTRODUCTION TO OPERATING SYSTEM SECUEIRY **10 Hrs.**

System Security Planning, Operating Systems Hardening, Security Maintenance, Linux/Unix Security, Windows Security, Virtualization Security, Operating System Integrity.

UNIT 3 DATABASE SECURITY **10 Hrs.**

Relational Databases, Access Control, Statistical Database Security, Privacy. Software Security, Introduction, Characters and Numbers, Canonical Representations, Memory Management, Data and Code, Race Conditions, Defences.

UNIT 4 INTRUSION DETECTION AND PREVENTION **09 Hrs.**

Protection against Threats, intruders, Viruses and Worms, Malicious Software, Distributed Denial of Service Attacks. Introduction to Intrusion Detection, and Prevention. Types of Intrusion Detection Systems. Honeypots, Incident Monitoring and Response. Malware analysis.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understanding of advanced public key cryptography algorithms.
CO2- Explain the optimal way to organize information system security.
CO3- Develop basic understanding of various types of intrusion and protection against them.
CO4- Analyse relevant professional and research ethical problems related to securing information system.
CO5- Develop basic understanding of computer, data and system security.
CO6- Create solutions to real time problems.

TEXT/REFERENCE BOOKS

1. Dieter Gollmann, “Computer Security”, A John Wiley and Sons Ltd.
2. Silbersehatz A. and Peterson J. L., “Operating System Concepts”, Wiley.
3. ElmasriRamez and NovatheShamkant, “Fundamentals of Database Systems”, Benjamin Cummings Publishing. Company.
4. Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw-Hill Education
5. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
6. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security: Private Communication in a Public World”, Prentice Hall

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS510P					Advanced Computer Security Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study principals in computer security.
- To study UNIX security.
- To study database security.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping guidelines and subject syllabus in mind.

1. Study and practice Internet Security in conventional operating systems: Memory, time, file, object protection requirements and techniques.
2. Study and practice security management - Attacks and Attackers, Risk and Threat Analysis.
3. Study and Practice identification and authentication mechanisms- Username and Password, Bootstrapping Password Protection, Protecting the Password File, Guessing Passwords , Phishing, Spoofing, and Social Engineering, Single Sign-on.
4. Study and practice Software Security: Characters and Numbers, Canonical Representations, Memory Management, Data and Code, Race Conditions, Defences.
5. Study trusted operating system security policies & models.
6. Implement program to solve some problems with the help of number theory algorithms.
7. Study and Install Intrusion Detection Tools like Snort.
8. Learn intrusion detection techniques using Snort.
9. Learn intrusion prevention technique.
10. Study and Practice malware analysis tools.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understanding of advanced number theory algorithms.
CO2- Explain the optimal way to organize information system security.
CO3- Develop basic understanding of various types of intrusion and protection against them.
CO4- Analyse relevant professional and research ethical problems related to securing information system.
CO5- Develop basic understanding of computer, data and system security.
CO6- Create solutions to real time problems.

TEXT/REFERENCE BOOKS

1. Dieter Gollmann, “Computer Security”, A John Wiley and Sons Ltd.
2. Silbersehatz A. and Peterson J. L., “Operating System Concepts”, Wiley.
3. ElmasriRamez and NovatheShamkant, “Fundamentals of Database Systems”, Benjamin Cummings Publishing. Company.
4. Behrouz A. Forouzan, “Cryptography and Network Security”, McGraw-Hill Education
5. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Prentice Hall.
6. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security: Private Communication in a Public World”, Prentice Hall

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS511T					Authentication Protocols in Cyber Space					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To understand mathematical foundations for authentication protocols.
- To study authentication architecture.
- To study existing authentication schemes.

UNIT 1 INTRODUCTION TO CYBERSPACE **10 Hrs.**

Communication protocol, Sensing, Actuations, IoT Applications domains,Security Issues In cyber layers, Security Architecture of cyberspace.

UNIT 2 MATHEMATICAL FOUNDATION **10 Hrs.**

Elliptic curve cryptography forAuthentication, Optimization techniques for ECC, Deffie-Hellman protocol, uni-factor and Multi-factor authentication schemes.

UNIT 3 AUTHENTICATION ARCHITECTURE FOR CYBERSPACE **10 Hrs.**

Threat Model for Authentication, End to End Authentication, Classification of Authentication techniques, Cyberspace Layered Authentication, Authentication requirements for Cloud centric Cyber Environment, Authentication requirements for resource constrained devices.

UNIT 4 AUTHENTICATION SCHEMES FOR CYBERSPACE **09 Hrs.**

Public key based Authentication, Identity basedauthentication encryption, Dynamic Identity based authentication encryption, RFID based authentication techniques,andBiometricbased authentication techniques.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to
CO1- Define security requirements in cyber space.
CO2- Explain authentication issues in cyber space.
CO3- Apply mathematical models in cyber space.
CO4- Analyse authentication models in cyber space.
CO5- Determine authentication schemes in cyber space.
CO6- Create authentication schemes in cyber space.

TEXT/REFERENCE BOOKS

1. C Patel, N Doshi, “Internet of Things Security: Challenges, Advances, and Analytics”, CRC Press, Taylor and Francis Group.
2. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”.Chapman& Hall/CRC.
3. ShancangLi,Li Da Xu, “Securing the Internet of Things”, Elsevier.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS511P					Authentication Protocols in Cyber Space Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand mathematical foundations for authentication protocols.
- To study authentication architecture.
- To study existing authentication schemes.

LIST OF EXPERIMENT

Experiment Sessions using Programming would be based on following topics:

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping guidelines and subject syllabus in mind.

1. Study Basics of Cybercrime investigation process.
2. Implement various authentication schemes for cyber security.
3. Implement authentication protocol for IoT applications.
4. Develop authentication algorithms for specific applications like IoT application, Cloud application, etc.
5. Study and implement authentication schemes for cyber security related latest research papers.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Define security requirements in cyber space.
CO2- Explain authentication issues in cyber space.
CO3- Apply mathematical models in cyber space.
CO4- Analyse authentication models in cyber space.
CO5- Determine authentication schemes in cyber space.
CO6- Create authentication schemes in cyber space.

TEXT/REFERENCE BOOKS

1. C Patel, N Doshi, “Internet of Things Security: Challenges, Advances, and Analytics”, CRC Press, Taylor and Francis Group.
2. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”. Chapman& Hall/CRC.
3. ShancangLi,Li Da Xu, “Securing the Internet of Things”, Elsevier.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS512T					Cyber Attacks and Defence					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study defence mechanism for cyber-attacks.
- To understand framework for security.
- To study cyber threats in real world.

UNIT 1 INTRODUCTION TO CYBER ATTACKS **10 Hrs.**

Security Posture: The current threat landscape, The credentials – authentication and authorization, Cyber security challenges, Incident Response Process.

UNIT 2 UNDERSTAND CYBER SECURITY CHAIN **10 Hrs.**

Understanding the cyber security Kill Chain, Internal reconnaissance, External reconnaissance, Access and privilege escalation, Sustainment, Threat life cycle management, Analysing current trends, Exploiting a vulnerability.

UNIT 3 BASIC SECURITY FRAMEWORKS **10 Hrs.**

Understanding Basic Security Frameworks, Security Policy, Policy enforcement, Network Segmentation, Securing remote access to the network, Virtual network segmentation, Hybrid cloud network security, Threat Intelligence.

UNIT 4 INCIDENT RECOVERY **09 Hrs.**

Examining Cyber Threats More Closely, Investigating an Incident, Investigating a compromised system on-premises, The disaster recovery planning process.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understanding of cyber defence and attack methods.
CO2- Determine software vulnerabilities and security solutions to reduce the risk of exploitation.
CO3- Apply various tools of cyber security.
CO4- Compare various cyber security measures.
CO5- Measure the performance and troubleshoot cyber security systems.
CO6- Design operational and strategic cyber security strategies and policies.

TEXT/REFERENCE BOOKS

1. ErdalOzkaya, Yuri Diogenes, "Cybersecurity - Attack and Defense Strategies", Packt Publishing.
2. Aditya Sood Richard Enbody, "Targeted Cyber Attacks", Elsevier
3. Edward G. Amoroso , "Cyber Attacks: Protecting National Infrastructure", Elsevier
4. Andy Jones,DebiAshenden, "Risk Management for Computer Security: Protecting Your Network & Information Assets", 1st Edition, Elsevier.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS512P					Cyber Attacks and Defence Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study defence mechanism for cyber-attacks.
- To understand framework for security.
- To study cyber threats in real world.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping guidelines and subject syllabus in mind.

1. Study and practice cyber-attacks tools.
2. Study and practice cyber defence strategies.
3. Practice vulnerability assessment tools.
4. Develop disaster recovery process for specific case studies.
5. Study and implement cyber-attacks and defence related latest research papers.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understanding of cyber defence and attack methods.
CO2- Determine software vulnerabilities and security solutions to reduce the risk of exploitation.
CO3- Apply various tools of cyber security.
CO4- Compare various cyber security measures.
CO5- Measure the performance and troubleshoot cyber security systems.
CO6- Design operational and strategic cyber security strategies and policies.

TEXT/REFERENCE BOOKS

1. ErdalOzkaya, Yuri Diogenes, “Cybersecurity - Attack and Defense Strategies”, Packt Publishing.
2. Aditya Sood Richard Enbody, “Targeted Cyber Attacks”, Elsevier
3. Edward G. Amoroso , “Cyber Attacks: Protecting National Infrastructure”, Elsevier
4. Andy Jones,DebiAshenden, “Risk Management for Computer Security: Protecting Your Network & Information Assets”, Elsevier.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS513T					Privacy in Cyber Network					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To study privacy in cyber and its impact.
- To study various leaks in cyber network.
- To study policy for cyber network.

UNIT 1 INFORMATION COMMUNICATION TECHNOLOGY **10 Hrs.**

ICT, and the Internet - email, chat, blogs, Skype and the Web; Social media - multidimensional communications. Crowd participation and crowd sourcing. Spread of information instantaneous.

UNIT 2 SOCIAL MEDIA **10 Hrs.**

Governance of Social Media. Freedom of speech and expression issues. Impact on National security. Economic value of data: personal data on SM platforms. Content control. Breaking news on SM, not TVs or newspapers: veracity of sources. Democratic governments – Social media threat.

UNIT 3 REGULATION **10 Hrs.**

Self-regulation. Content takedown. ICT impact on society, individuals, governments, war, revolutions: WikiLeaks. Indian Social Media Network.

UNIT 4 PRIVACY PROTECTION **09 Hrs.**

Larger picture: cybersecurity, privacy protection. Global Surveillance by US NSA – privacy violation of global citizens, their personal data on SM platform. Role of SM in future conflicts.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to
CO1- Understand the privacy in cyber network.
CO2- Demonstrate issues related to privacy in cyber network.
CO3- Identify standards of professionalism in cyber network.
CO4- Compare privacy in cyber network principals.
CO5- Determine the legal and technical aspects of a privacy.
CO6- Create the application of privacy in cyber network.

TEXT/REFERENCE BOOKS

1. Eric Schmidt and Jared Cohen; "the New Digital Age", Printed in India by Gopsons Papers Ltd., Noida.
2. Plotkin, "Privacy, Security, and Cyberspace (Computers, Internet, and Society)", Facts on File Inc.
3. Patrick Doreian, FransStokman, "Evolution of Social Networks", Routledge
4. John Scott, "Social Network Analysis", SAGE

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS513P					Privacy in Cyber Network Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To study privacy in cyber and its impact.
- To study various leaks in cyber network.
- To study policy for cyber network.

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Study privacy issues on different social media platform.
2. Study Facebook, YouTube and Twitter allow everyone to post messages of any kind, upload photographs and videos of anyone. How to view such 'publishing'? Which laws applicable?
3. Study Freedom of speech and expression issues.
4. Study ICT impact on society, individuals, governments, war, revolutions: WikiLeaks.
5. Study and implement privacy in cyber space related latest research papers.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the privacy in cyber network.
CO2- Demonstrate issues related to privacy in cyber network.
CO3- Identify standards of professionalism in cyber network.
CO4- Compare privacy in cyber network principals.
CO5- Determine the legal and technical aspects of a privacy.
CO6- Create the application of privacy in cyber network.

TEXT/REFERENCE BOOKS

1. Eric Schmidt and Jared Cohen; "the New Digital Age", Printed in India by Gopsons Papers Ltd., Noida.
2. Plotkin, "Privacy, Security, and Cyberspace (Computers, Internet, and Society)", Facts on File Inc.
3. Patrick Doreian, FransStokman, "Evolution of Social Networks", Routledge
4. John Scott, "Social Network Analysis", SAGE

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

20CS514T					Software Quality Assurance					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To understand organizational security.
- To study software quality policy.
- To study software auditing framework.

UNIT 1 ORGANIZATIONAL SECURITY **10 Hrs.**

Organizational Security, Security frameworks; Security Policy, Security standards, Security controls. ISO 27001 standard, ISMS and PDCA Approach; ISO 27013 changes

UNIT 2 CONCEPT OF TRUSTED SYSTEM

Confidentiality Policies (Bell-LaPadula Model), Integrity Policies (Biba& Clark-Wilson), Hybrid Policies (Chinese wall model), Other Formal Models for Computer Security, The Concept of Trusted Systems, Application of Multilevel Security, Trusted Computing. **10 Hrs.**

UNIT 3 IT SECURITY MANAGEMENT **10 Hrs.**

IT Security Management, Security Risk Assessment, Risk assessment methodologies like OCTAVE. Implementation of Controls, Security controls, security auditing; Monitoring Risks; Security policy enforcement – automated tools.

UNIT 4 SECURITY AUDIT **09 Hrs.**

Security Auditing Architecture, Audit Trail Analysis, Security breach management, legal compliance; The Economics of Cyber security, Modelling Cybersecurity.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the use of Security Quality Assurance.

CO2- Explain necessity of risk analysis

CO3- Apply practical knowledge of a variety of ways to test software and an understanding of some of the trade-offs between testing techniques.

CO4- Discover the reason for bugs and analyse the principles in software testing to prevent bugs.

CO5- Compare the software testing techniques in commercial environment.

CO6- Design various test processes for quality improvement.

.**TEXT/REFERENCE BOOKS**

1. Sandra Senft, Frederick Gallegos and Aleksandra Davis, “Information Technology Control and Audit, Fourth Edition”, CRC Press.
2. Daniel Galin, Software Quality Assurance : From Theory to Implementation, Addison Wesley, 2003.
3. Manish Agrawal, Alex Campoe and Eric Pierce, “Information Security and IT Risk Management”, Wiley

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks

Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS514P					Software Quality Assurance Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand organizational security.
- To study software quality policy.
- To study software auditing framework

LIST OF EXPERIMENT

Following list gives some programming examples. Faculty can prepare their own list in same manner keeping above guidelines and syllabus in mind.

1. Study frameworks and standards like PCI-DSS, SANS Controls.
2. Study risk assessment methodologies like OCTAVE.
3. Study Security Auditing Architecture.
4. Study the Economics of Cyber security, Making a Business Case, Quantifying Security, Modelling cyber security.
5. Study IT Act 2000, ITAA2008 & associated policies, procedures & guidelines. Regulatory compliance challenges; demonstrating due diligence in the event of breaches.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the use of Security Quality Assurance.

CO2- Explain necessity of risk analysis

CO3- Apply practical knowledge of a variety of ways to test software and an understanding of some of the trade-offs between testing techniques.

CO4- Discover the reason for bugs and analyse the principles in software testing to prevent bugs.

CO5- Compare the software testing techniques in commercial environment.

CO6- Design various test processes for quality improvement.

TEXT/REFERENCE BOOKS

1. Sandra Senft, Frederick Gallegos and Aleksandra Davis, “Information Technology Control and Audit, Fourth Edition”, CRC Press.
2. Daniel Galin, Software Quality Assurance : From Theory to Implementation, Addison Wesley, 2003.
3. Manish Agrawal, Alex Campoe and Eric Pierce, “Information Security and IT Risk Management”, Wiley.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks

Part B: Viva Examination based conducted experiments 50 Marks

20CS515T					Machine Learning in Cyber Security					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To understand the concepts of machine learning for cyber security.
- To learn how machine learning can be used to solve various security issues.
- To learn how to implement machine learning algorithms for cyber security.

UNIT 1 INTRODUCTION **08 Hrs.**

Why Machine Learning (ML) and Security: Cyber Threat Landscape, The Cyber Attacker's Economy, What Is ML, Real-World Uses of ML in Security, Spam Fighting: An Iterative Approach, Limitations of ML in Security

Classifying and Clustering: ML: Problems and Approaches, Training Algorithms to Learn, Supervised Classification Algorithms, Practical Considerations in Classification, Clustering

UNIT 2 ANOMALY DETECTION WITH ML

Anomaly Detection: Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection, Response and Mitigation. **09 Hrs.**

UNIT 3 ANALYSIS WITH ML

Malware Analysis: Understanding Malware, Feature Generation, From Features to Classification. **12 Hrs.**

Network Traffic Analysis: Theory of Network Defense, Machine Learning and Network Security, Building a Predictive Model to Classify Network Attacks.

UNIT 4 PRODUCTION SYSTEMS AND ADVERSARIAL ML

Production Systems: Defining Machine Learning System Maturity and Scalability, Data Quality, Model Quality, Performance, Maintainability, Monitoring and Alerting, Security and Reliability, Feedback and Usability. **10 Hrs.**

Adversarial Machine Learning: Terminology, The Importance of Adversarial ML,Security Vulnerabilities in Machine Learning Algorithms.

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the role of machine learning for cyber security.

CO2- Apply clustering techniques for anomaly detection.

CO3- Classify the malicious activities in the network/system using classification techniques.

CO4- Apply feature engineering techniques for malware analysis

CO5- Compare the supervised, semi-supervised and unsupervised techniques for network analysis.

CO6- Define maturity and scalability of security machine learning system.

.TEXT/REFERENCE BOOKS

1. Clarence Chio& David Freeman, "Machine Learning & Security: Protecting Systems with Data and Algorithms", O'Reilly.
2. Daniel Barbará, Sushil Jajodia, "Applications of Data Mining in Computer Security", Springer.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks

Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

20CS515P					Machine Learning in Cyber Security Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand the concepts of machine learning for cyber security.
- To learn how machine learning can be used to solve various security issues.
- To learn how to implement machine learning algorithms for cyber security.

LIST OF EXPERIMENT

Practical list should be prepared based on the content of the subject and following guidelines should be useful. Experiment Sessions using Programming would be based on following topics:

1. Implement data cleaning strategies
2. Use supervised learning for signature detection,
3. Use Decision tree classifier techniques to identify new attack patterns.
4. Use Probabilistic Learning for anomaly detection.
5. Use Classification techniques for spam detection.
6. Build a predictive model to classify network attacks.
7. Implement K-means cluserting techniques for network analysis.
8. Study and implement any research paper on Security machine learning system and measure its efficiency

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Understand the role of machine learning for cyber security.

CO2- Apply clustering techniques for anomaly detection.

CO3- Classify the malicious activities in the network/system using classification techniques.

CO4- Apply feature engineering techniques for malware analysis

CO5- Compare the supervised, semi-supervised and unsupervised techniques for network analysis.

CO6- Define maturity and scalability of security machine learning system.

TEXT/REFERENCE BOOKS

1. Clarence Chio& David Freeman, “Machine Learning & Security: Protecting Systems with Data and Algorithms”, O’Reilly.
2. Daniel Barbará, Sushil Jajodia, “Applications of Data Mining in Computer Security”, Springer.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks

Part B: Viva Examination based conducted experiments 50 Marks

22CS501T					Introduction to Blockchain Technology					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	--	--	100

COURSE OBJECTIVES

- To understand the concepts of distributed consensus and trust management.
- To understand the design principles of the block chains.
- To design and implement the distributed ledger and the smart contracts.

UNIT 1 INTRODUCTION TO BASICS OF BLOCKCHAIN **08 Hrs.**

Introduction to Blockchain, Building blocks: SHA 256, Peer to Peer Network, Distributed Ledger, Block mining, Proof of work, Miners and incentive mechanisms, Merkle tree, case-study applications of block chain framework: Bitcoin and transactions

UNIT 2 CONSENSUS AND CRYPTOCURRENCY

Proof-of-Work based consensus mechanisms, Proof of Stake based Chains, Types of Blockchain. Introduction to Crypto Currency, Crypto Currency as application of blockchain technology **09 Hrs.**

UNIT 3 SMART CONTRACT AND ETHEREUM

Ethereum Framework: Introduction, smart contract, Messages and transaction, state transition function, gas, applications, Solidity programming language: smart contract design, Rinkeby testnet **12 Hrs.**

UNIT 4 APPLICATIONS OF BLOCKCHAIN

Blockchain Use Cases – Finance, Industry, E-Governance and other contract enforcement mechanisms. Security and Research Aspects in Blockchain **10 Hrs.**

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Define the role of Blockchain technology in digitization.
CO 2- Illustrate the cryptographic concepts, distributed concepts, and smart contracts related to Blockchain technology.
CO 3- Experiment with Ethereum and Hyperledger framework for Blockchain development.
CO 4- Analyze the need of Blockchain for real life system.
CO 5- Choose the appropriate cryptographic primitives, type of Blockchain, mining method, and framework according to Blockchain usecase.
CO 6- Create the smart contracts and Blockchain for suitable system.

TEXT/REFERENCE BOOKS

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
2. White papers of Bitcoin, Ethereum, IOTA and Neo frameworks and research papers as communicated in the class.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

22CS501P					Introduction to Blockchain Technology LAB					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand the concepts of distributed consensus and trust management.
- To understand the design principles of the block chains.
- To design and implement the distributed ledger and the smart contracts.

LIST OF EXPERIMENT

Practical list should be prepared based on the content of the subject and following guidelines should be useful. Experiment Sessions using Programming would be based on following topics:

1. Create a Simple Blockchain in any suitable programming language.
2. Use Geth to Implement Private Ethereum Block Chain.
3. Memory Hard algorithm - Hashcash implementation
4. Direct Acyclic Graph Implementation
5. Puzzle mining implementation
6. Smart Contracts Creation
7. Create Case study of Block Chain being used in illegal activities in real world.
8. Using Python Libraries to develop Block Chain Application.

COURSE OUTCOMES

On completion of the course, student will be able to

CO1 - Define the role of Blockchain technology in digitization.
CO 2- Illustrate the cryptographic concepts, distributed concepts, and smart contracts related to Blockchain technology.
CO 3- Experiment with Ethereum and Hyperledger framework for Blockchain development.
CO 4- Analyze the need of Blockchain for real life system.
CO 5- Choose the appropriate cryptographic primitives, type of Blockchain, mining method, and framework according to Blockchain usecase.
CO 6- Create the smart contracts and Blockchain for suitable system.

TEXT/REFERENCE BOOKS

3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
4. White papers of Bitcoin, Ethereum, IOTA and Neo frameworks and research papers as communicated in the class.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 2 Hrs**

Part A: Evaluation Based on the class performance and Laboratory book 50 Marks
Part B: Viva Examination based conducted experiments 50 Marks

23CS501T					Web Penetration Testing					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	0	0	3	3	25	50	25	-	-	100

COURSE OBJECTIVES

- To understand the concepts and methodologies of web penetration testing.
- To learn about web application security.
- To learn various web application vulnerabilities and exploitation techniques.
- To develop skills for performing web penetration testing.

Unit 1. Introduction to web application security **9 Hrs.**

Introduction to security in web applications and common web application vulnerabilities; Web architecture and protocols: Understanding how web applications work, including HTTP requests and responses, cookies, sessions, and other web-related concepts; Web application technologies; Information gathering techniques

Unit 2. Active Enumeration and Vulnerability Identification **10 Hrs.**

Active enumeration for gathering information: Port scanning, Checking username validity, Brute forcing usernames, Enumerating files, Brute forcing passwords, Gathering other information from web pages; Identifying vulnerability: Automated URL-based directory traversal, automated cross-site scripting, query checking; Case studies

Unit 3. Web SQL Injection and Header Manipulation **11 Hrs.**

SQL Injection: Checking jitter, URL-based SQL injection, blind SQL injection, encoding payloads; Web Header Manipulation: Fingerprinting servers, testing for insecure headers, brute forcing login; testing for insecure cookie flags; session fixation through cookie injection; Case studies

Unit 4. Steganography, Encryption and Encoding in Websites **9 Hrs.**

Image Analysis and Manipulation: Hiding a message by steganography,extracting the hidden message, hiding text in image, extracting text from images, command and control by using steganography; Encryption and Encoding: Encoding with different techniques, cracking different ciphers, attacking one-time pad reuse; Case studies

Max. 39 Hrs.

COURSE OUTCOMES

On completion of the course, student will be able to

CO 1: Understand about security concerns in web applications.
CO 2: Learn the concepts and methodologies for penetration testing of a web application.
CO 3: Evaluate the security of a web application.
CO 4: Identify and exploit common web application vulnerabilities.
CO 5: Apply the skills to conduct web penetration testing.
CO 6: Develop effective mitigation strategies.

REFERENCE BOOKS

1. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", by Dafydd Stuttard (Author), Marcus Pinto: Wiley.
2. "Mastering Modern Web Penetration Testing", by Prakhar Prasad: Packt Publishing Limited.
3. "Web Application Security: A Beginner's Guide", by Bryan Sullivan and Vincent Liu: McGraw-Hill.
4. “Python Web Penetration Testing Cookbook”, by Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May, Dave Mound: Packt Publishing Limited.

END SEMESTER EXAMINATION QUESTION PAPER PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: 10 Questions of 2 marks each-No choice 20 Marks
Part B: 2 Questions from each unit with internal choice, each carrying 20 marks 80 Marks

23CS501P					Web Penetration Testing Lab					
Teaching Scheme					Examination Scheme					
L	T	P	C	Hrs/Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
0	0	2	1	2	-	-	-	50	50	100

COURSE OBJECTIVES

- To understand the concepts and methodologies of web penetration testing.
- To learn about web application security.
- To learn various web application vulnerabilities and exploitation techniques.
- To develop skills for performing web penetration testing.

Proposed List of Experiments

1. Working with HTTP requests and responses
2. Brute forcing passwords
3. Gathering other information from web pages
4. Automated cross-site scripting
5. URL-based SQL injection
6. Web Header Manipulation
7. Generate/Implement different hashes
8. Text/Image Steganography in Websites
9. Encoding with different techniques for Websites
10. Implementing an existing research work on web pentesting
11. Case studies on web pentesting
12. Mini Project/Literature review

COURSE OUTCOMES

On completion of the course, student will be able to

CO 1: Understand about security concerns in web applications.
CO 2: Learn the concepts and methodologies for penetration testing of a web application.
CO 3: Evaluate the security of a web application.
CO 4: Identify and exploit common web application vulnerabilities.
CO 5: Apply the skills to conduct web penetration testing.
CO 6: Develop effective mitigation strategies.

REFERENCE BOOKS

1. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", by Dafydd Stuttard (Author), Marcus Pinto: Wiley.
2. "Mastering Modern Web Penetration Testing", by Prakhar Prasad: Packt Publishing Limited.
3. "Web Application Security: A Beginner's Guide", by Bryan Sullivan and Vincent Liu: McGraw-Hill.
4. “Python Web Penetration Testing Cookbook”, by Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May, Dave Mound: Packt Publishing Limited.

END SEMESTER EXAMINATION PROPOSED PATTERN

Max. Marks: 100 **Exam Duration: 3 Hrs**

Part A: LAB Work-Continuous Evaluation 50 Marks
Part B: End-semester Practical Exam and Viva 50 Marks

3rd Semester

PANDIT DEENDAYAL ENERGY UNIVERSITY GANDHINAGAR

SCHOOL OF TECHNOLOGY

COURSE STRUCTURE FOR M. TECH - CYBER SECURITY													
Semester III			**M. Tech. - Cyber Security**										
Sr. No.	**Course/Lab Code**	**Course/Lab Name**	**Teaching Scheme**					**Examination Scheme**					
			L	**T**	**P**	**C**	**Hrs./Week**	**Theory**			**Practical**		**Total**
								CE	**MS**	**ES**	**CE**	**ES**	**Marks**
1	20CS611	Seminar				5		--	40	60			100
2	20CS612	Project				14		--	40	60			100
		Industrial Training											NP/PP
		TOTAL				19			80	120			200

CE- Continuous Evaluation, MS-Mid Semester; ES – End Semester Exam

4th Semester

PANDIT DEENDAYAL ENERGY UNIVERSITY GANDHINAGAR

SCHOOL OF TECHNOLOGY

COURSE STRUCTURE FOR M.TECH - CYBER SECURITY													
Semester IV			**M. Tech. - Cyber Security**										
Sr. No.	**Course/Lab Code**	**Course/Lab Name**	**Teaching Scheme**					**Examination Scheme**					
			L	**T**	**P**	**C**	**Hrs./Week**	**Theory**			**Practical**		**Total**
								CE	**MS**	**ES**	**CE**	**ES**	**Marks**
1	20CS621	Seminar				5		--	40	60			100
2	20CS622	Project and Dissertation				24		--	40	60			100
		TOTAL				29			80	120			200

CE- Continuous Evaluation, MS-Mid Semester; ES – End Semester Exam