M. TECH - CYBER SECURITY

TIFAC-Centre Of Relevance and Excellence (CORE) in Cyber Security

2021-2023

Cyber security is a very fast moving field. A program in security that aims to be on the forefront has to necessarily have a companion-advanced program that has a good balance between theoretical and practical aspects, analytical methods and system architectures, academic ideas and industry practices.

The Centre for Cyber Security was identified by TIFAC (Department of Science and Technology, Govt. of India) as a CORE in Cyber Security in September 2005. The TIFAC CORE gives significant thrust to the frontier areas of Cyber Security, including technology, practice, management, and policy issues. Research areas of the TIFAC CORE are organized into four broad categories, namely: Enterprise Wide Security, Data Center Security, Language-Based Security, and Hardware and Embedded Systems Security. These categories represent four horizontal layers of security in a typical information system /network that a practitioner would normally encounter in today's industrial settings and corporate environments. CORE also focuses on theory and practice of authentication, authorization, and access control techniques.

This M. Tech program provides a good blend of theory and industrial practice; necessary theoretical background, insight into general and technical aspects of Cyber Security, analytical methods and management practices in the field of Cyber Security are the areas receiving detailed attention. It aims at moulding the student into an Information Security professional. Practicing industry professionals and enterprise experts with little or no knowledge in Cyber Security too can benefit from this program.

Program Specific Objectives

1. The program aims at moulding the student into an ethical Cyber Security Professional.

2. The program will impart disciplinary and/or interdisciplinary technical knowledge & skills needed to protect computer systems from vulnerabilities, detect & respond to security breaches and cyber threats of all kinds

3. The skills imparted through the program can be used to perform cyber security risk assessment, troubleshoot performance issues, offer information assurance which can be applied immediately in their workplace or research areas viz.

Program Outcomes

1. Capabilities: Protect IT assets by designing/developing cyber security architecture, strategies and policies.
2. Research skills: experimental, computational, theoretical, practical - plan, implement, and monitor cyber security mechanisms.
3. Innovation: Identify, analyze, and remediate computer security breaches using innovative methods.
4. Real World Challenges: Analyze and evaluate cyber security needs of an organization; Conduct cyber security risk assessment; Measure performance issues and troubleshoot cyber security systems.

5. Employability: Be able to use cyber security, information assurance, and related tools applied immediately in their workplace or research areas.
6. Scholarship: ability to conduct independent and innovative research (and/or apply an interdisciplinary approach).
7. Communication skills: be able excel in delivering oral, written & presentation skills to various audiences.
8. Teaching skills: Knowledge, skills and ample opportunities to utilize their innate teaching skills.
9. Professional skills: Collaborative skills, ability to write grants & articles for journals and succeed in various competitive and professional certifications in the field of cyber security.
10. Ethical standards: Educational, personal and professional conduct and research.

CURRICULUM

First Semester

Course Code	Type	Course	L T P	C
21MA601	FC	Mathematical Foundations for Cyber Security	3 1 0	4
21CY602	FC	Concepts in System Security	3 0 0	3
21CY603	FC	Cryptography	3 0 3	4
21CY681	SC	Internet Protocol lab	0 0 6	2
	E	Elective 1		3
21CY682	SC	Secure Coding lab	0 0 6	2
21HU601	HU	Amrita Values Program		P/F
21HU602	HU	Career Competency I		P/F
				Credits 18

Second Semester

Course Code	Type	Course	L T P	C
21CY621	SC	Cyber Forensics	2 0 3	3
21CY622	SC	Applied Cryptography	3 0 3	4
21CY623	SC	Network Security	3 0 0	3
21CY624	SC	Web Application Security	2 0 3	3
	E	Elective II		3
21CY683	SC	Cyber Security Lab	0 0 6	2
21HU603	HU	Career Competency II	0 0 2	1
21RM615	SC	Research Methodology	1 0 0	1
				Credits 20

Third Semester

Course Code	Type	Course	L T P	C
	E	Elective III		3
	E	Elective IV		3
21CY798	P	Dissertation I		10
				Credits 16

Fourth Semester

Course Code	Type	Course	L T P	C
21CY799	P	Dissertation II		16
				Credits 16

Total Credits: 70

List of Courses

Foundation Core

Course Code	Course	L T P	C
21MA601	Mathematical Foundations for Cyber Security	3 1 0	4
21CY602	Concepts in System Security	3 0 0	3
21CY603	Cryptography	3 0 3	4

Subject Core

Course Code	Course	L T P	C
21CY621	Cyber Forensics	2 0 3	3
21CY622	Applied Cryptography	3 0 3	4
21CY623	Network Security	2 0 3	3
21CY624	Web Application Security	2 0 3	3
21RM615	Research Methodology	1 0 0	1

Laboratory

Course Code	Course	L T P	C
21CY681	Internet Protocol Lab	0 0 6	2
21CY682	Secure Coding Lab	0 0 6	2
21CY683	Cyber Security Lab	0 0 6	2

Course Code	Course	L T P	C
21RM615	Research Methodology	1 0 0	1

Electives

Course Code	Course	L T P	C
	Elective I		
21CY701	Data Mining and Machine Learning in Cyber Security	2 0 3	3
21CY702	Design and Analysis of Algorithms	2 0 3	3
	Elective II		
21CY703	Security of Cyber Physical Systems	3 0 0	3
21CY704	Steganography and Program Obfuscation	2 0 3	3
21CY705	Cryptographic Hardware and Embedded Systems	2 0 3	3
	Elective III		
21CY706	Coding and Information Theory	3 0 0	3
21CY707	Formal Methods for Security	3 0 0	3
21CY708	Android Security	2 0 3	3
21CY709	Wireless Networking and Security	2 0 3	3

	Elective IV		
21CY710	Security in Cloud Computing	2 0 3	3
21CY711	Special Topics in Cryptography	2 0 3	3
21CY712	Blockchain Technology	2 0 3	3
21CY713	Secure Systems Engineering	2 0 3	3
21CY714	Special Topics in Cyber Security	2 0 3	3

Project

Course Code	Courses	L T P	Cr
21CY798	Dissertation I		10
21CY799	Dissertation II		16

21MA601 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 3-1-0-4

Prerequisites:

Basics of Set Theory

Syllabus

Elementary Number Theory – Divisibility, Prime numbers, Arithmetic functions, Congruence, Quadratic Residues, Primitive roots, Algorithms for primality testing, Integer Factorization and Discrete Logarithm. Algebraic Structures - Groups, Rings, Fields and Lattices. Polynomials over Finite Field – Order of Polynomials, Primitive polynomials, Extension Fields, Vector space, Subspace, Inner product space, Orthogonalization, Diagonalization, Arithmetic of Elliptic Curves, Bilinear maps, Solving nonlinear system of equations using XL algorithm and Grobner basis techniques.

Text Book / References

1. R. Lidl and H. Niederreiter, *Finite Fields*, 2nd Edition, Cambridge University Press, 1997.
2. S.Y. Yan, *Number Theory for Computing*, 2nd Edition, Springer, Berlin, 2002.
3. G. Strang, *Introduction to Linear Algebra*, 4th Edition, Wellesley-Cambridge Press, 2009.
4. J. H . Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Dordrecht: Springer, 2009.
5. A. Joux, *Algorithmic Cryptanalysis*, Chapman & Hall/CRC Cryptography and Series, 2009.
6. Abijit Das, *Computational Number theory*, CRC Press, 2013.
7. Alko R. Meijer, *Algebra for cryptologists*, Springer, 2016.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understand the basic mathematical principles and functions that form the foundation for coding and cryptography.	**L1,L2,L3,L4**
CO 2	Understand basic concepts of various algebraic structures used in computer science.	**L2, L3, L5**
CO 3	Understand basic concepts of vector spaces and inner product spaces	**L2,L3**
CO 4	Application of linear algebra for image analysis and other applications	**L3,L4,L5**
CO 5	Understand basics of elliptic curves and its use for cryptographic applications	**L1, L2,L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	-	2	-	-	-	2	-	2	-	-	1	1	1
CO 2	-	2	-	-	-	2	-	2	-	-	1	1	1
CO 3	-	2	-	-	-	2	-	2	-	-	0	0	0
CO 4	-	2	-	-	-	2	-	2	-	-	0	1	0
CO 5	-	2	-	-	-	2	-	2	-	-	1	1	1

21CY602 CONCEPTS IN SYSTEM SECURITY 3-0-0-3

Prerequisites:

Basic knowledge on concurrency and access control. Practical experience in installation, monitoring, and troubleshooting of databases(*MySql, Oracle*) *and operating systems* (*Windows and Linux*)

Syllabus

Program vs processes, Transaction recovery and concurrency control in database systems. Access control mechanisms in general computing systems - Lampson's access control matrix. Mandatory access control, Authentication mechanisms in databases, DAC, MAC, RBAC, SELinux. Auditing in databases, Statistical inferencing in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases. Security and protection in operating systems - access control, auditing, trusted computing base with reference to Multics and the commercial Operating Systems. Malware analysis and protection- viruses, worms and Trojans, Rootkits, Ransomware, Polymorphic malware, Fileless malware, AI based malware, Malware capture and analysis using Honeypots, Ransomware Mitigation. Secure system configuration, Minimal footprint, Security of booting, Trusted computing, Virtualization techniques for security.

Text Book / References

1. Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in computing*, Prentice Hall Professional Technical Reference, 4th Edition, 2006.
2. M. Gertz and S. Jajodia, *Handbook of Database Security-Applications and Trends*, Springer, 2008.
3. T. Jaeger, *Operating System Security*, Vol. 1 of Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers, 2008.
4. W. Mauerer, *Professional Linux Kernel Architecture*, John Wiley and Sons, New York, 2008.
5. R Anderson, *Security engineering*, John Wiley & Sons, 2008.
6. Matt Bishop, *Computer security: Art and Science*, Vol. 2, Addison-Wesley, 2012.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Familiarity with terminology of database, software and system security	**L1**
CO 2	Exploring the access control security models and policies in database and operating systems	**L2**
CO 3	Familiarize the challenges, attacks and defences in database Systems	**L3/L4/L5**
CO 4	Exploring the basic functionalities of different types of malwares	**L2**
CO 5	Familiarize the challenges, attacks and defences in operating systems	**L3/L4/L5**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3

CO 1	1	2	2	2	2	2	-	1	2	-	1	1	1
CO 2	2	3	3	2	3	2	-	1	2	-	2	2	2
CO 3	3	3	3	2	3	2	-	1	2	-	2	2	2
CO 4	3	3	3	2	3	2	-	1	2	-	2	2	2
CO 5	3	3	3	2	3	2	-	1	2	-	2	2	2

21CY603 CRYPTOGRAPHY 3-0-3-4

Prerequisites: *Elementary Number Theory, Arithmetic functions, Congruence, Algebraic Structures - Groups, Rings, Fields*

Stream ciphers: Pseudo-random generators, Attacks on the one time pad, Linear generators, Cryptanalysis of linear congruential generators, The subset sum generator, Block ciphers: Pseudorandom functions and permutations (PRFs and PRPs), PRP under chosen plaintext attack and chosen ciphertext attack, Case study: *DES, AES, modes of operation*. Message integrity: Cryptographic hash functions, message authentication code, CBC MAC and its security, Cryptographic hash functions based MACs, Case study: *SHA512, SHA3, Merkle trees*. Authenticated Encryption-Authenticated encryption ciphers from generic composition, Public key encryption: RSA, Rabin, Knapsack cryptosystems, Diffie-Hellman key exchange protocol, ElGamal encryption, Elliptic curve cryptography. Digital signatures: Generic signature schemes, RSA, ElGamal and Rabin's signature schemes, blind signatures, threshold signature schemes, ECDSA, Signcryption.

Text Book / References

1. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
2. O. Goldreich, *Foundations of Cryptography:* Vol. 1, *Basic Tools*, Cambridge University Press, 2001.
3. O. Goldreich, *Foundations of Cryptography:* Vol. 2, *Basic Applications*, Cambridge University Press, 2004.
4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2007.
5. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice*, Pearson Education India, 2009.
6. Abijit Das, *Computational Number theory*, CRC Press, 2013.
7. Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*, V 0.5, 2020

	Course Outcome	Bloom's Taxonomy Level
CO 1	Achieving the goal of perfectly secure encryption and semantically secure encryption	**L1,L2**
CO 2	The inner workings of cryptographic systems and how to correctly use them in real-world applications.	**L2,L3,L4**
CO 3	How to prevent modification of non-secret data	**L2,L3,L4**
CO 4	Efficient and secure key management based on public-key cryptosystem	**L1,L3,L5**
CO 5	Validation of the authenticity and integrity of a message, software or digital document.	**L5,L6**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	2	1	2	1	-	1	2	-	1	1	1
CO 2	1	2	2	1	2	1	-	1	2	-	2	2	2
CO 3	1	2	2	1	2	1	-	1	2	-	2	2	2
CO 4	1	2	2	1	2	1	-	1	2	-	2	2	2
CO 5	1	2	2	1	2	1	-	1	2	-	2	2	2

21CY682 SECURE CODING LAB 0-0-6-2

Prerequisites: *C programming and Operating Systems*

Syllabus:

Security Concepts - SetUID - Environmental variables and Attacks - Shellshock attack - Common String Manipulation Errors and Vulnerabilities - Stack overflow, Off-by-one vulnerabilities, Return-to-libc, ROP - Integer Vulnerabilities - Memory management errors - Format string vulnerabilities - Concurrency and File I/O - Race conditions - Dirty COW Attack- Rules and recommendations of SEI CERT C coding Standards.

Text Book / References

1. Wenliang Du, *Computer Security – A hands-on Approach*, First Edition, Createspace Independent Pub, 2017
2. Robert C. Seacord, *The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems*, 2nd Edition, Pearson Education, 2016.

	Course Outcome	**Bloom's Taxonomy Level**
CO 1	Explore the working of system software and its common security threats	**L3**
CO 2	Identify and mitigate various system vulnerabilities	**L5**
CO 3	Create and test exploits for system vulnerabilities	**L5**
CO 4	Apply rules and recommendations from coding standards to develop secure software.	**L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	3	3	3	3	2	-	1	1	-	2	2	2
CO 2	2	3	3	3	3	2	-	1	1	-	3	3	3
CO 3	2	3	3	3	3	2	-	1	1	-	3	3	3
CO 4	2	3	3	3	3	2	-	1	1	-	3	3	3

21CY681 INTERNET PROTOCOL LAB 0-0-6-2

Prerequisite: *Basic knowledge about computer networks and troubleshooting of network systems*

Syllabus:

Familiarization with current generation network simulators: Installation and configuration of open-source simulators (ns2/ ns3), Creation of network topology and understanding of packet switched network, Simulation and visualization of different types of traffic-congestion controlled and non-congestion controlled, Trace analysis and visualization of protocol dynamics {throughput; packet drop, buffer dynamics, congestion window, round-trip-time, bandwidth delay product, receiver window, etc.}, Simulation with active queue management schemes. Familiarization of Networking tools with Linux: Configuring servers like samba and SMTP in Linux, Familiarization of tools like traceroute, netstat, nslookup, nc, Arp etc, and concepts of tcpdump, Wireshark, windump for packet capturing, analysis and visualization, Network emulation and traffic control using tc and dummynet, Network Programming: Implement a chat server that handles multiple clients using Java RMI, Simulation of link state and distance vector routing protocol using C Sockets, Basic Network Programming with python: Sockets, client programming, parsing of common file formats like CSV, HTML, XML and JSON, Implementation of a web application with frameworks like CGI and Django.

Text Book / References

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, Pearson Publication, 7th Edition, 2017.
2. L. Peterson and B. Davie, *Computer Networks: A Systems Approach*, 5th Edition, Elsevier Inc., 2011.
3. W. R. Stevens, *TCP/IP Illustrated, Vol.1: The Protocols*, Addison-Wesley, 1994.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Analyze network application services and protocols.	**L4**
CO 2	Illustrate data transfer and flow handling mechanisms for transport layer protocols.	**L3**
CO 3	Understand the working principle of routing mechanisms and analyze them for finding the shortest route.	**L4**
CO 4	Understand LAN design components, Network protocols and error handling code.	**L2**
CO 5	Understand the principles of network management.	**L2**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	3	3	3	2	2	-	1	2	-	2	2	2
CO 2	2	3	3	3	2	2	-	1	2	-	2	2	2
CO 3	2	3	3	3	2	2	-	1	2	-	2	2	2
CO 4	2	3	3	3	2	2	-	1	2	-	2	2	2
CO 5	2	3	3	3	2	2	-	1	2	-	2	2	2

21CY621 CYBER FORENSICS 2-0-3-3

Prerequisites: *CYXXX: Network Security*

Syllabus:

Locard's exchange principle, code of ethics, digital forensic process models of Lee, Carrier, Casey and Cohen. Framework for digital forensic evidence collection with Chain of Custody (CoC), standard evidence collection procedures (SOP). File carving with fundamentals of host forensics for windows artifacts, registry and system log monitoring with auditing mechanisms. File system handling - reconstruction of files and directory structures on the FAT and NTFS timestamps. Fundamentals of host forensics for unix derivatives - linux operating system forensics, epoch formats and audit mechanisms. Forensic analysis of database systems and identifying database tampering. Slack space forensics, swap space forensics, network device forensics, investigating logs, network traffic and web attacks, mobile device forensics, wireless forensics, anti-forensics, steganography, email investigation, social media forensics, investigating copiers, IVR, DVR and SIM cards. IPR and cyber laws in India, setting up a forensic laboratory, NIST tools (CFReDS, CFTT and NSLR).

Text Book / References

1. Brian Carrier, *File System Forensic Analysis*, Pearson, 2006.
2. E. Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.
3. Marjie T. Britz, *Computer Forensics and Cyber Crime*, Pearson, 2012.
4. David Cowen, *Computer Forensics: A Beginners Guide*, Mc Graw Hill Education, 2013.
5. Bill Nelson, Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations*, 4th Edition, 2014.

	Course Outcome	
CO 1	Exploring the fundamentals of host forensics for windows and Unix Systems	**L3/L4**
CO 2	Exploring the ideas of digital forensics framework	**L3/L4**
CO 3	Familiarizing the ideas of mobile and network system Forensics	**L3/L4**
CO 4	Exploring the ideas to Email and social Media forensics	**L2/L3**
CO 5	Familiarizing the fundamentals of anti-forensics and cyber laws	**L1/L2**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	-	2	3	2	2	1	-	-	2	-	1	1	1
CO 2	-	2	3	2	2	1	-	-	2	-	2	2	2
CO 3	-	2	3	2	2	1	-	-	2	-	2	2	2
CO 4	-	2	3	2	2	1	-	-	2	-	3	3	2
CO 5	-	2	3	2	2	1	-	-	2	-	3	3	3

21CY622 APPLIED CRYPTOGRAPHY 3-0-3-4

Prerequisites: *CYXXX Cryptography*

Syllabus:

Protocols for identification and login: Interactive protocols, Password protocols, Challenge-response protocols, Schnorr's identification protocol, zero-knowledge protocol. Authenticated Key Exchange: encryption-based protocol and its attacks, Perfect forward secrecy, Protocol based on ephemeral encryption, Attacks on insecure variations, Identity protection, One-sided authenticated key exchange, Security of authenticated key exchange protocols, Password authenticated key exchange. Key exchange protocol with trusted third party, Conference Key Protocols, Key Broadcasting Protocols.

Text Book / References

1. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography* , CRC Press, 1996.
2. J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of computer security* , Springer, 2003.
3. Abhijit Das and Veni Madhavan C. E., *Public-key Cryptography, Theory and Practice* , Pearson Education, 2009.
4. Colin Boyd, Anish Mathuria and Douglas Stebila,. *Protocols for Authentication and Key Establishment*, Springer, Berlin, Heidelberg, 2020
5. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Examine and analyze cryptographic protocols in existing systems.	**L1, L2,L4**
CO 2	Analyze Protocols for identification and login	**L2, L4, L5**
CO 3	Evaluation of Authenticated Key Exchange protocols	**L3, L4, L5, L6**
CO 4	Understanding the Conference Key Protocols and its applications	**L2,L4**
CO 5	Analyze of Key Broadcasting Protocols	**L2,L4**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	2	2	2	1	-	2	2	-	1	1	1
CO 2	1	2	2	2	2	1	-	2	2	-	1	1	2
CO 3	1	2	2	2	2	1	-	2	2	-	1	2	2
CO 4	1	2	2	2	2	1	-	2	2	-	1	2	1
CO 5	1	2	2	2	2	1	-	2	2	-	1	2	1

21CY624 WEB APPLICATION SECURITY 2-0-3-3

Prerequisites: *Basics of Web development* (*HTML. CSS, JavaScript, any Server side scripting language*)

Syllabus:

Threat Modeling – STRIDE. Risk Assessment - DREAD, Common Vulnerabilities and Exploits, CVSS scoring. Web Application Development and Security - OWASP Top 10 flaws - Web Application Technologies - Vulnerabilities - OS command injection - Directory traversal - SQL injection - Cross site Scripting (XSS) - Cross site Request Forgery (CSRF) - Clickjacking - Web Cache Poisoning - DOM based vulnerabilities - Access Control Vulnerabilities and Privilege Escalation - Cross-origin resource sharing (CORS) -- XML external entity (XXE) injection - Server-side request forgery (SSRF) - HTTP request smuggling - Web sockets security.

Text Book / References

1. Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.
2. Dafydd Stuttard, and Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd Edition, John Wiley & Sons, 2011.
3. Wenliang Du, *Computer Security – A hands-on Approach*, First Edition, Createspace Independent Pub, 2017
4. https://www.owasp.org

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understand and apply threat modelling technique to identify software vulnerabilities.	**L2**
CO 2	Identify and mitigate common server side security vulnerabilities	**L3**
CO 3	Identify and mitigate common client side security vulnerabilities	**L3**
CO 4	Apply standard mitigation technique to prevent security vulnerabilities.	**L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	2	2	3	1	-	1	1	-	2	2	2
CO 2	2	2	3	3	3	1	-	1	2	-	3	3	3
CO 3	2	2	3	3	3	1	-	1	2	-	3	3	3
CO 4	2	2	3	3	3	1	-	1	2	-	3	3	3

21CY623 NETWORK SECURITY 3-0-3-4

Prerequisites:

Basic knowledge about computer networks and troubleshooting of network systems.

Syllabus:

Networking Basics: Familiarization of Networking tools like traceroute, netstat, nslookup, nc, arp etc, Configuring servers like samba and SMTP in linux, Socket Programming with python; Techniques for Network Protection: Firewalls, packet filter and stateful firewalls, application aware firewalls, personal firewalls-iptables, Proxies, NAT, Intrusion Detection System-Snort, Signature and Anomaly based detection, Honeypots and Honeynets, Network Log management-syslog or SPLUNK; RBAC: Role mining; Network reconnaissance-Nmap and vulnerability audits-openVAS; DNS-Dig tool: DNS based attacks, Phishing-DNSTwist, DNSSEC-DS and NSEC records; Network based malware attacks: Remote access Trojan-Poison Ivy and Domain name generation algorithm based Botnets; LAN attacks: ARP Cache poisoning, MAC flooding, Man in the middle attacks, Port Stealing, DHCP attacks, VLAN hopping; Network Sniffing-Wireshark and Password Cracking-John the Ripper, tcpdump, windump; Secure Network Communication: SCP, SSH, SSL3.0, TLS 1.2, STARTTLS, IPSec, VPN and Secure HTTP; Understanding the dark web, TOR traffic, Attacks on SSL/TLS: SSL stripping, Drown and Poodle attack; Encrypting and Signing Emails: PGP- GPG/openPGP, DKIM and SPF; Single Sign On (SSO)-OAUTH and OPENID; Network packet creation and Manipulation using scapy and dpkt libraries; SDN Security.

Text Book / References

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Pearson edition, 2016
2. Vincent J. Nestler et. al, *Principles of computer security Lab Manual*, 4th Edition, McGraw-Hill, 2014
3. Behrouz A. Forouzan, *Cryptography & Network Security*, McGraw-Hill, 2007
4. C. Kaufman, R. Perlman and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall PTR, 2002.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understand various techniques for Network Protection and explore new tools and attacks in network security domain	**L2/L1**
CO 2	Exploring DNS based attacks and DNSSEC	**L2/L3**
CO 3	Familiarize the LAN based attacks and its mitigations	**L4**
CO 4	Exploring Secure Network Communication protocols and attacks	**L5**
CO 5	Exploring the protocols used for SSO and challenges, attacks related to Email communication	**L1/L4**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	2	3	3	-	-	1	2	-	2	2	2
CO 2	2	2	2	3	3	-	-	1	2	-	3	3	3
CO 3	2	2	3	3	3	-	-	1	2	-	3	3	3
CO 4	2	2	3	3	3	-	-	1	2	-	3	3	3
CO 5	2	2	3	3	3	-	-	1	2	-	3	3	3

21CY683 **CYBER SECURITY LAB** **0-0-9-3**

Prerequisite:

Basic network troubleshooting, OSI layers, Basic usage of Linux utility

Objectives

1. To configure virtual networks using network simulator
2. To install and exploit security tools for protecting a network
3. To implement cryptographic algorithm for building a secure communication network
4. To exploit the vulnerabilities in a LAN environment and launch attacks
5. To analyze the network packet using Wireshark
6. To perform the web penetration testing using Burp suite
7. To perform vulnerability assessment of wireless devices
8. To exploit vulnerabilities in the systems
8. To perform the log analysis using Splunk
9. To find vulnerable apps in play store and perform static and dynamic analysis on it

The experiments make use of Kali Linux distros and other open source security tools.

Experiment No. 1: LAN based Network Security

Set up a simple LAN as shown in Figure 1. M1-3 and S1-3 are machine which have Linux and Windows running.

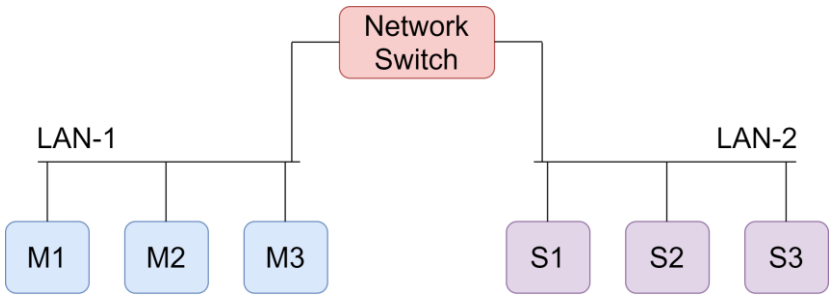

Figure 1: A Simple LAN environment

1. Configure LAN-1 and LAN-2 as separate VLANs in the network switch (use inter VLAN ACL).
2. Create a SPAN port in the network switch and send the mirrored traffic to a promiscuous mode port for the purpose of IDS and other packet analysis. Practice port based and VLAN based mirroring.
3. Familiarize with 802.1x, Network Admission Control, Microsoft NAP, RADIUS protocol, RADIUS per port ACL

Experiment No. 2: Network reconnaissance and Protection

1. Installing ‘iptable’ in Ubuntu VM to allow/block communication between VMs
   a) Installing Email server and Web server in VMs. Usage of Firewall (iptable) in blocking/allowing a sub-network from accessing the servers
   b) Configuring iptable to block Telnet inbound and outbound connections
2. Use ‘nmap’ tool to perform vertical and horizontal scanning for checking open and closed ports. Use nmap commands for performing the following experiments:
   a) Use ping sweeping to determine which hosts are running.
   b) Check for vulnerable services available using TCP connect scans.
   c) Perform OS Fingerprinting to determine the OS of target machine.
   d) Choose different options under each category according to your creativity.

Experiment No. 3: Application of Cryptographic algorithms using Crypto tools.
Establish a Client-Client Secure communication protocol as shown in Figure 2.

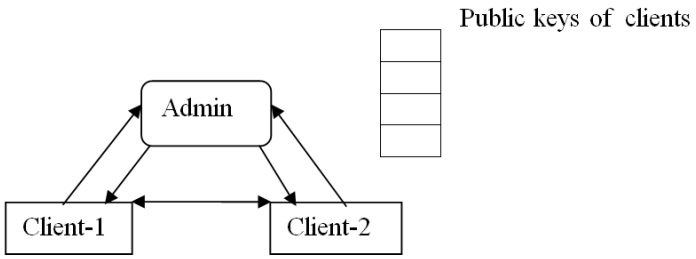

Figure 2: Secure Communication

The Client machines (Client-1 and Client-2) and Admin machine are installed in different VMs. All the three machines are interconnected through a network switch with different IP addresses. The Admin runs a program that generates 2048 bit RSA public and private key for a Client that wants to communicate. Admin generates 2048 bit RSA public and private key for Client-1 and Client-2. The private keys are distributed to client machines and public keys are stored in a structure in the admin machine. When Client-1 wants to send message to Client-2, it encrypts the messages with public key of Client-2. The message is decrypted by Client-2 with its private key. Similar communication pattern from Client-2 to Client-1 need to be maintained.

Manually capture the traffic between the hosts to ensure the proper working of the encryption. Construct an asynchronous communication between Client-1 and Client-2. Run a Wireshark/ TCPdump at the SPAN/Promiscuous port of the network switch and identify the communication between the communicating entities (Admin, Client-1, and Client-2).

Experiment No. 4: LAN based insider attacks

Make use of Ettercap/arpspoof tool to perform ARP cache poisoning based attacks in a LAN environment:
1. Perform Denial of Service (DoS) attacks using ARP Cache poisoning attacks
2. Perform DNS Spoofing attack using ARP Cache poisoning attacks
3. Perform Password stealing (over plaintext) using ARP Cache poisoning attacks
4. Invoke ‘sslstrip tool’ for stealing password from any machine that is connected in a LAN by stripping the https connection.

For all the above attacks, observe the ARP cache table, CAM table, etc., before and after the attack. Run Wireshark and observe the traffic patterns before and after the attack.

Experiment No. 5: Network Packet analysis using Wireshark.

Use Wireshark to solve the below scenarios:

1. You, as a SOC analyst noted that someone try to send information (PING) to unknown IP address and you are suspecting some malicious information might transferred in it. Analyse the log file and find the data.
   a) Find the source and destination IP of that log.
   b) Find the Data length (Bytes) and verify the checksum status on destination.
2. Now you have found that some kind of file is been downloaded by insider in unencrypted web traffic. Your task is to
   a) Find the type of file.
   b) Export that file from that web traffic, then analyse the file for any secret information.
   c) Find the hostname in which the file is stored.
3. Based upon their activities, auditing team has started investigation against them and found that the insider passed some sensitive information via call to someone. The traffic is been captured. Analyse the traffic and find those conversations and extract the sensitive information in it.
   a) Find the call-ID when the status of the call is ringing.
4. On further investigation, you have a suspect on some wireless device communications. List out the Bluetooth devices communications from this traffic and find the details about native Bluetooth adapter.
5. Analyse the captured WPA handshake from this traffic and report in detail about it to your administrator.
   a) Geo locate all the endpoint of wireless devices.
   b) Analyse the protocol level information transfer between wireless devices.

Experiment No. 6: Web Penetration testing using Burp Suite.

1. Configure burp suite in machine A and access the request and response going throw machine B. Both A and B machines should be pingable.
2. Intercept an https request through butpsuite using import/export CA certificates.
3. Intercept a web application login credentials using burpsuite and resend request using repeater.
4. Use intruder to bruteforce password list.

Experiment No. 7: Wireless Security Lab

Perform a VA/PT on your local Wi-Fi network and try automated attacks with NetStumbler and Kismat to gather information wireless network and try attacks like CowPatty and Airsnort. Further execute aircrack-ng to simulate attacks 802.11 WEP and WPA-PSK keys for auditing wireless networks and performing airodump, aircrack, airmon, airbase, aireplay and airtun using Kali 2.0 (Sana) Linux. Attempt a Wi-Fi sniffing to gather location data which can be used to identify device parameters of wireless communication devices.

Experiment No. 8: Exploiting the vulnerabilities on a system

Use Metasploit (open-source exploit framework) to write and test your own exploit into any PC/Site with existing payloads using Virtual Machines in Ubuntu Host and Windows XP Virtual disk. These traces should be executed in OllyDbg step by step, and debug the protocols every single command, laidback with registers and flags, with buffer information. Also debug standalone DLL's like Message Box and wsprintf. Use IDA Pro (evaluate a limited version of the disassembler) to examine a protected and obfuscated sample executable. (.NET Reflector can be used to search through, the class hierarchies of .NET assemblies, even without any source code). Perform static and dynamic code auditing.

Experiment No. 9 : Log analysis using Splunk

Understand the architecture of Splunk and installation process. Familiarize with the dashboard fields. Run any process in forwarder and use corresponding query to capture that log in Splunk. Run any malware of malicious process in forwarder, capture the log and analyze the malware using Splunk.

Experiment No. 10: Mobile & Smart phone security Lab
Familiarize with android application .apk files. By performing static and dynamic analysis on the app. Find the vulnerable application and document the inferences

	Course Outcome	Bloom's Taxonomy Level
CO 1	Implementation of various network exploits and its mitigation techniques using simulators and real devices	**L2/L1**
CO 2	To exploit vulnerabilities in LAN, wireless devices and identify the same using penetration testing	**L3/L4**
CO 3	Exploring the reverse engineering techniques for proper classification of Benign and malicious Desktop/ Android applications	**L3/L4**
CO 4	Implementation of Intrusion detection system by applying machine learning algorithms.	**L5**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	3	3	3	3	2	-	1	-	-	3	3	3
CO 2	2	3	3	3	3	2	-	1	-	-	3	3	3
CO 3	2	3	3	3	3	2	-	1	-	-	3	3	3
CO 4	2	3	3	3	3	2	-	1	-	-	3	3	3

21CY701 DATA MINING AND MACHINE LEARNING IN CYBER SECURITY 2-0-3-3

Prerequisites: *Statistics and Probability*

Syllabus:

Introduction to Data Mining and Machine Learning, Classical Machine learning paradigms for Data Mining, Fundamentals of Supervised and Unsupervised Machine Learning algorithms, Feature Selection – Methods. Machine learning for anomaly detection using Probabilistic Learning, Unsupervised learning,

Combination learners, Evaluation methods, Hybrid detection. Machine learning for network scan detection and Network traffic profiling, Deep Learning - Deep Feedforward Networks, Convolution Networks, Sequence Modeling - Recurrent and Recursive Nets, LSTM, Autoencoders, Deep Reinforcement learning. Representation Learning, Structured Probabilistic Models for Deep Learning, Deep Generative Models - Generative adversarial network and its variants, Applications in malware analysis and anomaly detection.

Text Book / References

1. Tom M Mitchell, *Machine Learning*, McGraw Hill, 1997.
2. Jiawei Han, Micheline Kamber, Jian Pei, *Data Mining: Concepts and Techniques*, 3rd edition, 2011.
3. D. K. Bhattacharyya and J. K. Kalita, *Network Anomaly Detection: A Machine Learning Perspective*, 1st Edition, Chapman and Hall/CRC, 2013.
4. T. Dunning and E. Friedman, *Practical Machine Learning - A New Look at Anomaly Detection*, O'Reilly, 1st edition, 2014.
5. Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep Learning*, MIT Press, 2016.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding various Machine Learning and Data Mining Techniques.	**L2/L1**
CO 2	Apply different Machine Learning Techniques for Cyber Security Problems like IDS.	**L3**
CO 3	Analyze various Feature extraction and reduction techniques	**L4**
CO 4	Evaluate the performance of various ML algorithms in Real time network environments.	**L5**
CO 5	Understand and apply Deep Learning techniques for Network security.	**L2/L3**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	-	2	2	2	2	3	-	1	1	-	1	2	1
CO 2	-	2	2	2	2	3	-	1	1	-	1	2	2
CO 3	-	2	2	2	2	3	-	1	1	-	1	2	2
CO 4	-	1	2	2	2	3	-	1	1	-	2	2	2
CO 5	-	2	2	2	2	3	-	1	1	-	2	2	2

21CY702 DESIGN AND ANALYSIS OF ALGORITHMS 2-0-3-3

Prerequisites:

Date Structures and Discrete Mathematics

Syllabus

Basic techniques for designing and analyzing algorithms, Dynamic programming, Divide and conquer, balancing, Upper and lower bounds on time and space costs, Worst case and expected cost measures,

Disjoint set, Graph algorithms, Persistent data structures, Polynomial complexity classes - P, NP, and co-NP, Intractable problems, Randomized data structure, Search Trees and Skip Lists, Online Algorithms - k-Server Problem, Stable Marriage Algorithm. Approximation Algorithms - Greedy Approximation Algorithms, Weakly Polynomial-time Algorithms, 3/2-approximation for TSP, ILP relaxations. Fixed Parameter Algorithms - Parameterized Complexity, Kernelization, Treewidth. Parallel Algorithms – Pointer Jumping and Parallel prefix. Amortized analysis, Fast Multiplication Algorithms, Number Theoretic algorithms, Polynomial and Matrix calculations, Pseudo polynomial time algorithms, Random number generators. Heap - Binomial, Fibonacci. Randomized Hashing- Universal Hashing, Perfect Hashing.

Text Book / References

1. R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.
2. D. E. Knuth, *Art of Computer Programming*, Vol. 3, *Sorting and Searching*, 2nd Edition, Addison-Wesley Professional, 1998.
3. T. Cormen, C. Leiserson, R. Rivest and C. Stein, *Introduction to Algorithms*, 3rd Edition, McGraw-Hill, 2009.
4. J. J. McConnell, *Analysis of Algorithms: An Active Learning Approach*, Jones & Bartlett Publishers, 2001.
5. S. Dasgupta, C. H. Papadimitriou and U. V. Vazirani, *Algorithms*, McGraw-Hill, 2008.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understand various methodology for analyzing algorithms.	**L2/L1**
CO 2	Discuss various NP problems and develop Polynomial Reduction algorithms for those problems.	**L2**
CO 3	Analyze various randomized, parallel and approximation algorithms, compare its computational efficiency.	**L4**
CO 4	Evaluate the performance of various Parameterized-fixed parameter algorithms and analyze the cost.	**L5**
CO 5	Apply various number theoretic and hashing algorithms in to cyber security applications and evaluate the performance .	**L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	-	-	1	1	1	1	-	1	1	-	1	1	0
CO 2	-	-	1	1	1	1	-	1	1	-	1	1	1
CO 3	-	-	1	1	1	1	-	1	1	-	1	1	1
CO 4	-	-	1	1	1	1	-	1	1	-	2	1	1
CO 5	-	-	1	1	1	1	-	1	1	-	2	1	1

21CY709 WIRELESS NETWORKING AND SECURITY 2-0-3-3

Prerequisite: *CYXXX Internet Protocol lab*

Syllabus:

Overview of Electromagnetic Theory and Propagation, Digital Modulation techniques, Signal Encoding Techniques, Spread Spectrum Techniques, Multiple Access, IEEE 802 standards. Cellular Concept, Standards, GSM Architecture, Handoff & Roaming, Interference, CDMA, 3G and 4G Systems, Satellite Networks & GPS, Wi-Max, Ultra Wide Band, IEEE 802.11 Standards, Bluetooth and other IEEE 802.15 standards. Threats to Wireless networks, Attacks on 802.11 networks – WEP, WPA, Wireless clients, Attacks on Bluetooth network, Eavesdropping, Privacy Challenges, Risks – Denial of Service, Insertion Attacks, Surveillance, War Driving, Jamming and Denial of Service. Authentication, Encryption/Decryption in GSMs. Securing the WLAN, WEP, RC4, WPA/ WPA2, IEEE 802.11i, Security in Bluetooth, Wi-MAX, UWB and Satellite networks, Android Security, 5G and security.

Text Book / References

1. Joshua Wright and Johnny Cache, *Hacking Exposed Wireless*, 3rd Edition: Wireless Security Secrets & Solutions, McGraw-Hill Education, 2015.
2. Jon Edney and William A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison-Wesley Professional,1st Edition, 2003.
3. H. Chaouchi and Maryline Laurent-Maknavicius, *Wireless and Mobile Networks Security*, Wiley, 2009.
4. K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall, 2002.
5. C. Peikari and S. Fogie, *Maximum Wireless Security*, Sams Publishing, 2002.
6. W. Stallings, *Wireless Communications and Networks*, 2nd Edition, Pearson Education Ltd, 2009.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understand the overview of Electromagnetic Theory and Propagation.	**L2/L1**
CO 2	Discuss cellular design concepts and various multiple access systems.	**L2**
CO 3	Analyze Threats to Wireless networks and Attacks on 802.11.	**L4**
CO 4	Understand various Attacks and mitigation strategy of Bluetooth network.	**L5**
CO 5	Analyze various Authentication, Encryption/Decryption in GSMs and Security in Wi-MAX, UWB and Satellite networks	**L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	1	1	1	1	2	-	1	1	-	1	1	1
CO 2	1	1	1	1	1	2	-	1	1	-	2	2	2
CO 3	1	2	2	3	3	2	-	1	1	-	3	3	3
CO 4	1	2	2	3	3	2	-	1	1	-	2	2	2
CO 5	1	2	2	3	3	2	-	1	1	-	3	3	3

21CY706 CODING AND INFORMATION THEORY 3-0-0-3

Prerequisites: *CYXXX: Mathematical Foundations for Cyber Security*

Syllabus:
Information theory- Information, Entropy, Discrete memoryless source, Source coding - Shannon-Fano coding, Huffman coding, Lempel-Ziv and arithmetic codes, Rate distortion theory, Optimum Quantizer Design. Discrete memoryless channel, Mutual information, Channel capacity, Shannon limit, Error control codes - Linear block codes, Error detection and correction, Hamming codes, Reed Muller codes, Golay codes, Cyclic codes, Binary BCH codes, Reed Solomon codes, Decoding algorithms, Trellis representation of codes, Convolution codes and its applications, Viterbi algorithm and decoding.

Text Book / References

1. R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press Cambridge, UK, 2003
2. S. Lin and D.J. Costello, *Error Control Coding - Fundamentals and Applications*, 2nd Edition, Pearson Education Inc., NJ., USA, 2004.
3. Elwyn R. Berlekamp, *Algebraic Coding Theory*: *Revised Edition*, World Scientific, 2015.
4. Thomas M. Cover, and Joy A. Thomas, *Elements of information theory*, John Wiley & Sons, 2012.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Knowledge of Source coding and channel performance using Information theory	**L1/L2**
CO 2	Comprehend various error control coding scheme	**L2/L4**
CO 3	Apply linear block codes for error detection and correction	**L3**
CO 4	Learn convolutional codes and cyclic codes for error detection and correction	**L4/L5**
CO 5	Design BCH and RS codes for Channel performance improvement against errors	**L3/L5/L6**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	-	1	1	-	-	1	-	2	-	-	0	0	0
CO 2	-	1	1	-	-	1	-	2	-	-	0	0	0
CO 3	-	1	1	-	-	1	-	2	-	-	0	0	0
CO 4	-	1	1	-	-	1	-	2	-	-	1	1	1
CO 5	-	1	1	-	-	1	-	2	-	-	1	1	1

21CY704 STEGANOGRAPHY AND PROGRAM OBFUSCATION 2-0-3-3

Prerequisites: *CYXX: Mathematical Foundations of Cyber Security*

Syllabus:
Steganography in images, Spatial and transform domain steganography: S-tool, J-Steg, OutGuess. Steganalysis, Basics of visual cryptography. Program Obfuscation - Methods of attack and defense, Program analysis: Static Analysis (Taint Analysis and Program Slicing), Dynamic Analysis (Profiling and Tracing). Familiarizing of the tools: Ghidra, IDA Pro, GDB Debugger. Code obfuscation- Complicating

control flow, Opaque predicates, Data encoding, Software Watermarking, Intellectual Property Protection: software birthmarking, software forensics, plagiarism detection, clone detection.

Text Book / References

1. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T.Kalker, *Digital Watermarking and Steganography*, 2nd Edition, The Morgan Kaufmann Series in Multimedia Information and Systems, 2002.
2. J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st Edition, Cambridge University Press, 2010.
3. C. Collberg and J. Nagra, *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*, Addison-Wesley, 2010.
4. M. T. Raggo and C. Hosmer, *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, 1st Edition, Syngress, 2012.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding various security issues in multimedia and provide secure measures through steganography	**L1**
CO 2	Analyzing the security of the stego systems using steganalysis techniques	**L2**
CO 3	Understand various code obfuscation methods	**L2**
CO 4	Analysis of obfuscated software using static and dynamic methods	**L3/L4**
CO 5	Understand various other IP protection methods	**L3**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	3	2	3	-	-	1	1	-	1	1	1
CO 2	1	2	3	2	3	-	-	1	1	-	1	1	1
CO 3	1	2	3	2	3	-	-	1	1	-	2	2	2
CO 4	1	2	3	2	3	-	-	1	1	-	2	2	2
CO 5	1	2	3	2	3	-	-	1	1	-	2	2	2

21CY703 SECURITY IN CYBER PHYSICAL SYSTEMS 3-0-0-3

Prerequisite: *CYXXX: Network Security*

Syllabus:

Introduction to Cyber Physical Systems: Standards, Topologies, Network Hardware, Network Standardization, Transmission Principles, Networked Systems and Internet structure: Introduction to the Internet and Cyber Physical application interface, basic concepts of the Internet Services and Protocols, higher level protocols, System Architecture of the Cyber-Physical Systems (CPS), Edge connectivity and protocols - Collaborative outsourcing in CPS, Sockets and Client/Server structures and wireless and wired P2P existing architectures, Hybrid and purely Mobile Peer-to-Peer Communication and principles, supported protocols and communication pros and cons, Wireless systems and CPS configuration and supported foundations and architectures, Cognitive CPS: efficiency, and resource manipulation, Wireless Sensor Network (WSN), life cycle, energy efficiency, lifetime of WSNs, energy conservation, Enabling Multimedia applications in Cyber-Physical Systems, Resource Sharing schemes and protocols, Cloud

Computing paradigm and the state-of-the-art methodologies, CPS and Edge Computing as a novel paradigm-Case studies

Text Book / References

1. Song, Houbing, et al., eds. Cyber-physical systems: foundations, principles and applications. Morgan Kaufmann, 2016.
2. Hofmann, Markus, and Leland R. Beaumont. Content networking: architecture, protocols, and practice. Elsevier, 2005.
3. Shahrestani, Seyed. "Internet of things and smart environments." Cham: Springer international (2018).
4. Wolf, Marilyn, and Dimitrios Nikolaou Serpanos. Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems. Springer, 2020.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding Standards and Topologies CPS	**L1,L2**
CO 2	Understanding the System Architecture of the CPS	**L2,L5**
CO 3	Collaborative outsourcing in CPS	**L3, L4**
CO 4	Understanding Wireless systems and CPS configuration and supported foundations and architectures	**L2,L3,L4**
CO 5	Cognitive CPS, Enabling Multimedia applications in CPS, CPS and Edge Computing	**L3,L5,L6**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	3	3	3	1	-	1	1	-	1	1	1
CO 2	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 3	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 4	2	2	3	3	3	1	-	1	1	-	3	3	3
CO 5	2	2	3	3	3	1	-	1	1	-	3	3	3

21CY705 CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS 2-0-3-3

Prerequisite: *CYXXX: Cryptography*

Introduction to Verilog- Structure, Constructs, and Conventions. Modeling at Gate level, Data flow level, Behavior level, and switch level. Design, Simulation, and Synthesis of digital circuits, Modules, and Systems. Functions, Tasks, User defined primitives, Compiler directives. Queues, PLAs, and FSMs. FPGAs – blocks inside, their features and use. IDE and its use, FPGA based design realizations, Design of finite field arithmetic operations, Representative designs with AES, ECC and Hash Algorithms.

Text Book / References

1. M. C. Cileti, *Advanced Digital Design with Verilog HDL*, Prentice Hall, 2002.
2. S. Brown and Z. Vranesic, *Fundamentals of Digital Logic with Verilog Design*, Tata McGraw Hill, 2002.

3. T. R. Padmanabhan and B. Bala Tripura Sundari, *Design through Verilog HDL*, IEEE Press, John Wiley, 2003.
4. F. Riodrigues-Henriquez, N. Saqib, A. Diaz-Perez and C. Koc, *Cryptographic Algorithms on Reconfigurable Hardware*, Springer, 2007.
5. C. K. Koc, *Cryptographic Engineering*, Springer, 2008.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Study verilog: structure, constructs, and conventions. Learn to model at gate level, data flow level, behavior level, and switch level	**L1/L2**
CO 2	Design, simulate and synthesis of digital circuits, modules, and systems. Understand the concepts of functions, tasks, user defined primitives, Compiler directives	**L2,L5**
CO 3	Gain the core idea of queues, PLAs, and FSMs. Learn the concepts of FPGAs - blocks inside, their features and use	**L2/L3**
CO 4	FPGA based design realizations	**L3/L5**
CO 5	Design of finite field arithmetic operations, Representative designs with AES, ECC and Hash Algorithms	**L5/L6**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	3	2	3	-	-	1	1	-	1	1	1
CO 2	2	2	3	2	3	-	-	1	1	-	1	1	1
CO 3	2	2	3	2	3	-	-	1	1	-	1	1	1
CO 4	2	2	3	2	3	-	-	1	1	-	2	2	2
CO 5	2	2	3	2	3	-	-	1	1	-	2	2	2

21CY707 FORMAL METHODS FOR SECURITY 3-0-0-3

Prerequisite: *Logic and Discrete Mathematics*

Syllabus:

Formal Methods – Propositional and Predicate logic, and theorem-proving, Fixed-points and their role in program analysis and model-checking, Verification of sequential programs using weakest preconditions and inductive methods, and verification of concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL), Application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols, Information flow and taint analysis for security of web applications, pi-calculus for formal modelling of mobile systems and their security. SPIN, PVS, TAMARIN, Frama-C and Isabelle tools.

Text Book / References

1. Edmund M. Clarke, Orna Grumberg and Doron Peled, *Model Checking*, MIT Press, 1999.

2. Lloyd, J.W., *Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic*, Springer Berlin Heidelberg, 2003.
3. M. Ruth and M. Ryan, *Logic in Computer Science - Modelling and Reasoning about Systems*, Cambridge University Press, 2004 .
4. G. Bella, *Formal Correctness of Security Protocols*, Springer, 2009.
5. Datta A, Jha S, Li N, Melski D and Reps T, *Analysis Techniques for Information Security*, Synthesis Lectures on Information Security, Privacy, and Trust, 2010.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Introduction to Formal Methods- Logic and Program Verification.	**L1**
CO 2	Understand Temporal Logic and Model Checking for program verifications.	**L2**
CO 3	Verification of concurrent and reactive programs/systems using model-checking and propositional temporal logic.	**L4**
CO 4	Application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols	**L3**
CO 5	Familiarizing SPIN, PVS, TAMARIN, Frama-C and Isabelle tools.	**L5**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	3	2	3	1	-	1	1	-	0	0	0
CO 2	1	2	3	2	3	1	-	1	1	-	1	1	1
CO 3	1	2	3	2	3	1	-	1	1	-	2	2	2
CO 4	1	2	3	2	3	1	-	1	1	-	2	2	2
CO 5	1	2	3	2	3	1	-	1	1	-	2	2	2

21CY708 ANDROID SECURITY 2-0-3-3

Prerequisites: *CYXXX: Secure Coding lab, CYXXX: Cyber Security lab*

Syllabus

App development- Activities, Intents, Fragments, Data storage, Broadcast receivers and Content Providers, Services, Async Tasks, GPS and GoogleMaps, Sensors, Connecting WebAPIs, Emulator and ADB, APK Internals, Networking, Device Rooting, TCP/IP Attacks, TCP/IP Attacks Using Android, DAC and MAC Permissions, Android Internals, Framework, Init, Zygote, Binder, Service Manager, Activity Manager, Reverse Engineering- Apktool, Ghidra, Jadx, Static and Dynamic analysis, Native Library Exploitation, OWASP, Security Assessment with Drozer and Burpsuite, Some of the attacks and Vulnerabilities in real world android apps (A case study) - XSS, Strandhogg, Code Injection -Overlay Attacks, Insecure Deeplinks, Malware Analysis, Bouncer, Privacy Violation, System Call Hardening, ASLR, ROP, Framework Exploits.

Text Book / References

1. Y. Karim, *Embedded Android*, Vol. 1, O'Reilly Media, 2013.
2. E. Nikolay, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2014.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Android Application development and APK internals	L6
CO 2	Understanding the internals of Android Mobile OS and study the architecture, design and security of mobile computing	L1/L2
CO 3	Exploring the Reverse Engineering tools and methodologies	L1/L3/L4
CO 4	Familiarize the attacks and Vulnerabilities in android apps	L2/L3
CO 5	Android Code Protection: Past, Present and Future Directions	L4/L5

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	3	3	3	1	-	1	1	-	1	1	1
CO 2	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 3	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 4	2	2	3	3	3	1	-	1	1	-	3	3	3
CO 5	2	2	3	3	3	1	-	1	1	-	3	3	3

21CY710 SECURITY IN CLOUD COMPUTING 2-0-3-3

Prerequisite: *CYXXX: Network Security*

Syllabus:

Introduction to distributed systems, Distributed computing paradigms, Inter process communication mechanisms, Process models in distributed systems, The CAP theorem, Consistency models and Replication, Consensus algorithm: Clock Synchronization – Logical clocks – Mutual Exclusion, global positioning of nodes, Distributed Commit protocols – 2PC, 3PC, Check-pointing and Recovery, Election algorithms, Failure Models, RAFT algorithm- Apache Zookeeper, Distributed file system – Eg: CODA and Ceph, Distributed storage implementation – Data sharding, NoSQL key value stores and its properties – Eg: Google Big Table, Amazon DynamoDB. Cloud computing benefits and its challenges, Types – Private, Public and Hybrid clouds, Models – IaaS, PaaS and SaaS. Cloud Security Patterns – 1. Secure Architecture 2. Compliance & Regulatory (GDPR, CCPA, HIPAA), 3. Identification, Authentication & Authorization 4. Secure Development, Operations & Administration 5. Policy & Confidentiality. Cloud - AWS, Azure, GCP. REST API services including load balancing, server authentication and debug handling, Hadoop cloud computing framework – HDFS and MapReduce, SPARK, Cloud data processing using Pig and Hive, Amazon EMR for creating Hadoop clusters within AWS.

Text Book / References

1. S. Ghemawat, H. Gobioff, and S. T. Leung, *The Google file system*, In ACM symposium on operating systems review, Vol. 37, No. 5, pp. 29-43, 2003.

2. J. Dean and S. Ghemawat, *MapReduce: simplified data processing on large clusters*, Commun., ACM 51, no.1, 107-113, 2008.
3. R. Chow, P. Golle, M. Jakobsson, R. Masuoka, Jesus Molina Elaine Shi and Jessica Staddon, *Controlling data in the cloud: outsourcing computation without outsourcing control*, In Proceedings of the ACM workshop on Cloud computing security, pp. 85-90, 2009.
4. T. Mather, S. Kumaraswamy and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* O'Reilly Series, 2009.
5. T. Erl, R. Puttini and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall, 2013.
6. M. Ben-Ari, *Principles of Concurrent and Distributed Programming*, Addison- Wesley/Pearson, 2nd Edition, 2006.
7. George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair, *Distributed Systems: Concepts and Design*, 5th Edition, 2011.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding the distributed systems, algorithms and protocols	**L1**
CO 2	Familiarization of distributed storage implementation	**L3**
CO 3	Evaluate Security in the cloud-infrastructure and analyze various attacks on cloud computing	**L5/L4**
CO 4	Understanding various cloud services and key management problems in cloud storage	**L2/L3**
CO 5	Exploring Hadoop cloud computing framework	**L3/L4**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	3	2	3	1	-	1	1	-	1	1	1
CO 2	1	2	3	2	3	1	-	1	1	-	2	2	2
CO 3	1	2	3	2	3	1	-	1	1	-	3	3	3
CO 4	1	2	3	2	3	1	-	1	1	-	3	3	3
CO 5	1	2	3	2	3	1	-	1	1	-	2	2	2

21CY711 SPECIAL TOPICS IN CRYPTOGRAPHY 2-0-3-3

Prerequisite: *CYXXX: Cryptography, CYXXX: Applied Cryptography*

Syllabus:

Lattice based cryptography - Integer lattices, Hard problems on lattices - Shortest vector problem, Code based cryptography, Hash based cryptography, Homomorphic encryption, BLS signatures, Group signatures, Identity based encryption, Broadcast encryption. Functional encryption.

Text Book / References

1. Daniele Micciancio and Shafi Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective* , 2002.

2. J. H . Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106, Dordrecht: Springer, 2009.
3. C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*, Springer, 2010.
4. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.
5. Peikert, C., *A decade of lattice cryptography*, Foundations and Trends in Theoretical Computer Science, 10(4), pp.283-424, 2016.
6. Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*,V4, 2017.
7. *Rings and Integer Lattices in Computer Science*, lectures notes from the Bellairs-McGill workshop on Computational Complexity in 2007.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding the NP hard problems on Lattices	**L1,L2**
CO 2	Understanding hardness of code based cryptography	**L2,L5**
CO 3	Understanding homomorphic encryption and its applications	**L4**
CO 4	Evaluation of Identity based cryptosystems	**L2,L3,L4**
CO 5	Understand the concepts of functional encryption	**L2,L3,L5,L6**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	1	2	2	1	2	1	-	1	2	-	0	0	0
CO 2	1	2	2	1	2	1	-	1	2	-	1	1	1
CO 3	1	2	2	1	2	1	-	1	2	-	1	1	1
CO 4	1	2	2	1	2	1	-	1	2	-	1	1	1
CO 5	1	2	2	1	2	1	-	1	2	-	1	1	1

21CY712 BLOCKCHAIN TECHNOLOGY 2-0-3-3

Prerequisites: CYXXX*: Cryptography*, CYXXX*: Network Security*, CYXXX*: Concepts in System Security*

Syllabus:

Blockchain Data structure, Hash chain, Distributed database, Index structure, Blockchain Architecture - Hashes, Transactions, Asymmetric-Key Cryptography, Addresses and Address Derivation, Private Key Storage, Ledgers, Blocks, Chaining Blocks. Consensus and multiparty agreements - Protocols, Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Elapsed Time, Deposit based consensus, Proof of importance, Federated consensus or Federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance. Blockchain implementation, Forking - Soft Fork, Hard Forks, Cryptographic Changes and Forks, Smart contract programing, Blockchain Platforms – Cryptocurrencies (Bitcoin, Litecoin, Ethereum, Ripple), Hyperledger, Ethereum. Blockchain - Outside of Currencies, IPFS protocol and Blockchain, Blockchain Concurrency and scalability, Network models and timing assumptions.

Text Book / References

1. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice*, Pearson Education India, 2009.
2. Melanie Swan, *Blockchain - Blueprint for a new economy*, O'Reilly Media, Inc., 2015.
3. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016
4. Roger Wattenhofer, CreateSpace, *The Science of the Blockchain*, Independent Publishing Platform, 2016
5. Imran Bashir, *Mastering Blockchain*, 2017.
6. Andreas M. Antonopoulos, *Mastering Bitcoin - Programming the Open Blockchain*, O'Reilly Media, Inc., 2017
7. Alex Leverington, *Ethereum Programming*, Packt Publishing Limited, 2017.
8. Draft NISTIR 8202, Blockchain Technology Overview - NIST CSRC, 2018.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding basic principles of distributed ledger technology	**L1, L2,**
CO 2	Use of cryptographic primitives in Blockchain technology	**L3,L4,L5**
CO 3	Evaluation of consensus protocols	**L2,L4,L5**
CO 4	Development of smart contracts	**L3,L4,L6**
CO 5	Blockchain and its use cases	**L2,L4,L5,L6**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	2	1	2	1	-	1	2	-	1	1	1
CO 2	2	2	2	1	2	1	-	1	2	-	1	1	1
CO 3	2	2	2	1	2	1	-	1	2	-	1	1	1
CO 4	2	2	2	1	2	1	-	1	2	-	2	2	1
CO 5	2	2	2	1	2	1	-	1	2	-	2	2	1

21CY713 SECURE SYSTEMS ENGINEERING 2-0-3-3

Prerequisite: *CYXXX Concepts in System Security*

Syllabus:

Information flow and vulnerability model to build security into life cycle phase of software (and hardware) components, Vulnerability analysis into architecture and design process, Access-controlled and clean environment to build software, Target environment hardening and secure application deployment, Attack trees, Security testing: SAST, DAST, IAST, Pen Testing, fuzzing. Software security economics - logging/monitoring and physical and operational security aspects. DevSecOps – Cloud (AWS, GCP, Azure), Cluster (Kubernetes), Container (Docker), Continuous Security, Integration and Continuous Delivery (CS/CI/CD), Introduction to hardware security – Physical and side channel attacks and its

countermeasures, Tamper resistance, Balancing security and usability – User authentication mechanisms, Secure browsing, Social media and data sharing, Countermeasures for possible social engineering attacks in design, Secure interactive design, Privacy issues in Human Computer Interaction.

Text Book / References

1. S. Garfinkel and L. F. Cranor, *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly, 2008.
2. Bird, Jim. "DevOpsSec: *Securing software through continuous delivery*." (2016).
3. Tim Mather, Subra Kumaraswamy, Shahed: *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly, 2009.
4. Anderson, Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2010.
5. M. Tehranipoor, and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.
6. C. W. Axelrod, *Engineering Safe and Secure Software Systems*, Artech House, 2013.
7. Antonio Borghesi and Barbara Gaudenzi: *Risk Management: How to Assess, Transfer and Communicate Critical Risks*, Springer, 2013.
8. Steve Watkins: *An Introduction to Information Security and ISO27001:2013: A Pocket Guide*, 2nd Edition, IT Governance Publishing, 2013.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding various information flow and vulnerability model to build security into life cycle phase of software components	**L2**
CO 2	Understanding various hardware security	**L2**
CO 3	Apply Vulnerability analysis into architecture and design process, access-controlled and clean environment to build software, target environment hardening and secure application deployment	**L3**
CO 4	Connecting the security and usability – User authentication mechanisms, secure browsing, social media and data sharing. Countermeasures for possible social engineering attacks in design. Secure interactive design. Privacy issues in Human Computer Interaction. Security Economics	**L1**
CO 5	Understanding security tools and practices in continuous delivery	**L5**

CO-PO Mapping													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	3	3	2	3	2	-	1	2	-	2	2	2
CO 2	2	3	3	2	3	2	-	1	2	-	3	3	3
CO 3	2	3	3	2	3	2	-	1	2	-	3	3	3
CO 4	2	3	3	2	3	2	-	1	2	-	3	3	3
CO 5	2	3	3	2	3	2	-	1	2	-	3	3	3

21CY714 SPECIAL TOPICS IN CYBER SECURITY 2-0-3-3

Prerequisites: *CYXXX: Network Security, CYXXX: Concepts in System Security*

Syllabus:

Information Technology and IPR, Intellectual Property Law, privacy law and data protection, Privacy issues in citizen digital data, lockers, electronic voting, digital cash, health and other societal digital information, Information & cyber warfare, social engineering attacks, Quantum computers, cyber security during crisis & pandemic, detection of fake news & misinformation, cyber attacks on ICS & critical infrastructure, state-level cyber operations & cyber weapons, threat detection & response, Digital trust & safety, digital privacy & ethics, ethics in cyberspace, Information Protection Bill, data security governance, Supply-chain attacks, Password less & hardware based authentication, Ethical hacking tools & techniques, Significant case studies & hands-on experience using tools / packages for each module, IDPR, trans-border data flow issues.

References

1. Easttom, Chuck. Computer security fundamentals. Pearson IT Certification, 2019.
2. Whyte, Christopher, A. Trevor Thrall, and Brian M. Mazanec, eds. Information Warfare in the Age of Cyber Conflict. Routledge, 2020.
3. Stuttard, Dafydd, and Marcus Pinto. The web application hacker's handbook: Finding and exploiting security flaws. John Wiley & Sons, 2011.
4. Look, Burt G. Handbook of SCADA/control systems security. CRC Press, 2016.
5. Eddison, Leonard. Tor And The Deep Web: The Complete Guide To Stay Anonymous In The Dark Net. CreateSpace Independent Publishing Platform, 2018.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding privacy law & data protection, trans border data flow issues	**L1,L2**
CO 2	Understanding the social engineering attacks, supply-chain attacks	**L2,L5**
CO 3	Cyber-attacks on ICS & critical infrastructure	**L4**
CO 4	Understanding data security governance, Information Protection Bill	**L2,L3,L4**
CO 5	Hands-on experience in Ethical hacking tools & techniques	**L3,L5,L6**

CO-PO Mapping

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO1	PSO2	PSO3
CO 1	2	2	3	3	3	1	-	1	1	-	1	1	1
CO 2	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 3	2	2	3	3	3	1	-	1	1	-	2	2	2
CO 4	2	2	3	3	3	1	-	1	1	-	3	3	3
CO 5	2	2	3	3	3	1	-	1	1	-	3	3	3