M. TECH - CYBER SECURITY

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

2024

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
24MA601	FC	Mathematical Foundations for Cyber Security	2 0 0	2
24CY602	SC	Network Security	3 0 0	3
24CY603	FC	Cryptography	3 0 3	4
24CY681	SC	Internet Protocol lab	0 0 6	2
24CY604	SC	Web Application Security	3 0 3	4
24CY605	SC	Secure Coding	2 0 3	3
22AVP103	HU	Mastery Over Mind	1 0 2	2
23AVP601	HU	Amrita Values Program*		P/F
23HU601	HU	Career Competency I		P/F
				Credits 20

Second Semester

Course Code	Type	Course	L T P	C
24CY611	SC	Cyber Forensics	2 0 3	3
24CY612	SC	Applied Cryptography	3 0 3	4
24CY613	FC	Concepts in System Security	2 0 3	3
	E	Elective I		3
	E	Elective II		3
24CY682	SC	Cyber Security Lab	0 0 6	2
23HU611	HU	Career Competency II	0 0 3	1
24RM600	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
24CY798	P	Dissertation-I		10
				Credits 16

Fourth Semester

Course Code	Type	Course	L T P	C
24CY799	P	Dissertation-II		16
				Credits 16

Total Credits: 72

List of Courses

Foundation Core

Course Code	Course	L T P	C
24MA601	Mathematical Foundations for Cyber Security	2 0 0	2
24CY613	Concepts in System Security	2 0 3	3
24CY603	Cryptography	3 0 3	4

Subject Core

Course Code	Course	L T P	C
24CY611	Cyber Forensics	2 0 3	3
24CY612	Applied Cryptography	3 0 3	4
24CY602	Network Security	3 0 0	3
24CY604	Web Application Security	3 0 3	4
24CY605	Secure Coding	2 0 3	3
24RM600	Research Methodology	1 0 0	1

Laboratory

Course Code	Course	L T P	C
24CY681	Internet Protocol Lab	0 0 6	2
24CY682	Cyber Security Lab	0 0 6	2

Electives

Course Code	Course	L T P	C
	Elective I		
24CY731	Data Mining and Machine Learning in Cyber Security	2 0 3	3
24CY732	Cryptographic Hardware and Embedded Systems	2 0 3	3
	Elective II		
24CY741	Security of Cyber Physical Systems	3 0 0	3
24CY742	Steganography and Malware Analysis	2 0 3	3
	Elective III		
24CY751	Coding and Information Theory	3 0 0	3
24CY752	Formal Methods for Security	2 0 3	3
24CY753	Mobile Security	2 0 3	3
24CY754	Wireless Networking and Security	2 0 3	3
	Elective IV		
24CY761	Security in Cloud Computing	2 0 3	3
24CY762	Special Topics in Cryptography	3 0 0	3
24CY763	Block chain Technology	2 0 3	3
24CY764	Secure Systems Engineering	2 0 3	3
24CY765	Special Topics in Cyber Security	3 0 0	3

Project

Course Code	Courses	L T P	Cr
24CY798	Dissertation-I		10
24CY799	Dissertation-II		16

24MA601 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 2-0-0-2

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

24CY613 CONCEPTS IN SYSTEM SECURITY 2-0-3-3

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- processes- Binaries-Libraries- Concurrency control in OS and databases- Statistical inferencing in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases- Access control in OS and databases- Access control Models - DAC- MAC- RBAC- SELinux – Sandboxing- SetUID Programs, Environmental variable based Attacks - Shellshock attack- Process memory organization- Stack management- Stack overflow - Runtime protection strategies, Return-to-libc, ROP, Format string vulnerabilities - File I/O Race conditions - TOCTOU - Dirty COW Attack - Virtualization techniques for security - Malware and its mitigation strategies- viruses, worms and Trojans- Rootkits- Ransomwares- Polymorphic malware- Fileless malware- AI-based malware- Packers - Trusted computing- TEE - SIEM- Auditing in Databases and OS- Zero Trust Security.

Text Book / References

1. Wenliang Du, *Computer Security – A hands-on Approach*, First Edition, Createspace Independent Pub, 2017
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	**L2**
CO 2	Exploring the access control security models and policies in database and operating systems	**L3**
CO 3	Familiarize the challenges, attacks and defences in database Systems	**L4**
CO 4	Exploring the basic functionalities of different types of malwares	**L4**
CO 5	Familiarize the challenges, attacks and defences in operating systems	**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	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

24CY603 **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

24CY605 **SECURE CODING** **2-0-3-3**

Prerequisites: *C programming and Operating Systems*

Syllabus:

Gauging the threat- Bugs- CWE- CVE - Strings - Common String Manipulation errors - Improperly Bounded String Copies - Off-by-One Errors - Null-Termination Errors - String Truncation - String Errors without Functions - String vulnerabilities - Safe String handling functions. Dynamic Memory Management - C Memory management functions - Common C Memory Management Errors - Initialization Errors - Failing to Check Return Values - Dereferencing Null or Invalid Pointers - Referencing Freed Memory - Freeing Memory Multiple Times - Memory Leaks - Zero-Length Allocations - Mitigation Strategies. Integer Security - Introduction to Integer Types - Integer Data Types - Integer Conversions - Integer Operations - Integer Vulnerabilities -Mitigation Strategies. Formatted Output - Variadic Functions - Formatted Output Functions - Vulnerabilities - Mitigation Strategies. Concurrency - Common Errors - Race Condition Vulnerabilities - Mitigation Strategies. Rules and recommendations of SEI CERT C coding Standards. Secure coding with C++, Java and Python.

Secure Data Structures - Arrays and Linked lists- Secure Stack- Secure Queue-Binary search Tree -Merkle Tree- Hash Tables - Bloom filter - Complexity.

Text Book / References

1. Goodrich MT, Tamassia R, Goldwasser MH. Data Structures and Algorithms in Java. Sixth edition, John Wiley & Sons Ltd; 2014.
2. Seyedeh Setareh Ghorshi. SafeDS: Safe Data Structures for C++, 2022.
3. Robert C. Seacord, *The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems,* 2nd Edition, Pearson Education, 2016.
4. CERT C Coding Standard.

   Available online: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard.

	Course Outcome	**Bloom's Taxonomy Level**
CO 1	Identify and mitigate the vulnerabilities based on integer operations and errors in formatted output.	**L3**
CO 2	Identify and mitigate the vulnerabilities due to string manipulation errors and dynamic memory management errors.	**L3**
CO 3	Secure Coding with C++, Java and Python	**L4**
CO 4	Implementation of Safe Data structure algorithms	**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	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

24CY681 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. Configuring servers like Samba and SMTP in Linux, Familiarization of tools like *traceroute, netstat, nslookup, nc*, *tcpdump*, *Wireshark, windump,* parsing and analysis of protocols like HTTP, TCP/IP, DHCP, ARP, Wi-Fi, DNS etc., 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 server programming.

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	Trace analysis and visualization of protocol dynamics	**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 and Network protocols	**L3**
CO 5	Network Programming with C, Java and Python	**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	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

24CY611 **CYBER FORENSICS** **2-0-3-3**

Prerequisites: *CYXXX: Network Security*

Syllabus:

Locard's exchange principle, code of ethics, digital forensic process models- Framework for digital forensic evidence collection with Chain of Custody (CoC), standard evidence collection procedures (SOP), *Autopsy*, Device/SSD forensics, 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, Password Cracking. Fundamentals of host forensics for UNIX derivatives - Linux operating system forensics, epoch formats and audit mechanisms, Mac forensics, Forensic analysis of database systems, and identifying database tampering. Slack and swap space forensics, Android and iOS forensics, memory, *volatility* and network forensics, wireless forensics, anti-forensics, steganography, email investigation, social media forensics, Cloud Forensics, Overwriting/Forging/Wiping/Destruction, IVR, DVR, NIST tools (CFReDS, CFTT, and NSLR).

Self-study: OSINT, Online Anonymity and Rootkits, Financial Frauds, Espionage and Investigations, investigating copiers, AI-assisted trends in cyber forensics

Text Book / References

1. Brian Carrier, *File System Forensic Analysis*, Pearson, 2006.
2. Nina Godbole, Sunit Belapure, *Cyber security: understanding cybercrimes, computer forensics and legal perspectives*, Wiley, 2011
3. E. Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.
4. Marjie T. Britz, *Computer Forensics and Cyber Crime*, Pearson, 2012.
5. David Cowen, *Computer Forensics: A Beginners Guide*, Mc Graw Hill Education, 2013.
6. 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**
CO 2	Exploring the ideas of digital forensics framework	**L3**
CO 3	Familiarizing the ideas of device and network system Forensics	**L4**
CO 4	Exploring the ideas to Email and social Media forensics	**L4**
CO 5	Familiarizing the fundamentals of anti-forensics and mobile forensics	**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	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

24CY612 **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. encryption-based protocol and its attacks, Perfect forward secrecy, Protocol based on ephemeral encryption, Attacks on insecure variations-Downgrade attack, Identity protection, One-sided authenticated key exchange, Security of authenticated key exchange protocols, Authenticated Key Exchange/PAKE. Key exchange protocol with trusted third party, Conference Key Protocols, Key Broadcasting Protocols, Federated Identity/SSO.

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

24CY604 WEB APPLICATION SECURITY 3-0-3-4

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

Syllabus:

Web Application Development basics - client side- server side technologies- session management techniques- 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, API security issues. Web 3.0 Architecture and 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 the fundamentals of web applications	**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

24CY602 **NETWORK SECURITY** **3-0-0-3**

Prerequisites:

Basic knowledge about computer networks and troubleshooting of network systems.

Syllabus:

Techniques for Network Protection: Firewalls, packet filter and stateful firewalls, application aware firewalls, personal firewalls, Proxies, NAT, Intrusion Detection System-Snort, Signature and Anomaly based detection- Evasion and poisoning attacks, Honeypots and Honeynets, Network Log management-syslog or SPLUNK; RBAC, Network reconnaissance-Nmap and vulnerability audits-*openVAS*; DNS-*Dig* tool: DNS based attacks, Phishing, 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, Password Cracking-*John the Ripper* ; 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

Self Study: Security of SCADA, TCP/IP interface protocols and security/vulnerability issues, Dark Web analysis, ICS and IoT

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**
CO 2	Exploring DNS based attacks and DNSSEC	**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	**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

24CY682 CYBER SECURITY LAB 0-0-6-2

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 with *Metasploit*
9. To perform the log analysis *Wazuh, Splunk*
10. Incident Monitoring using *Security Onion*

The experiments make use of Linux 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.

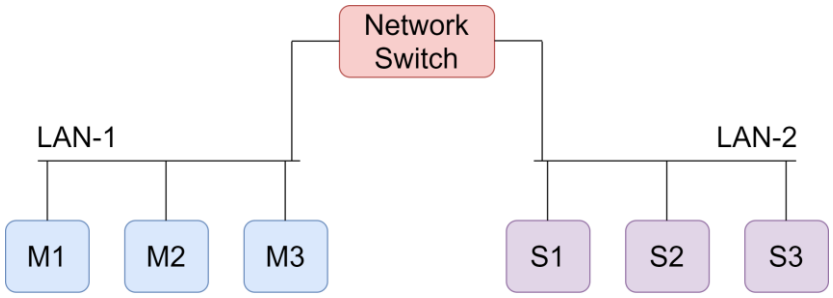

Figure 1: A Simple LAN environment

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.

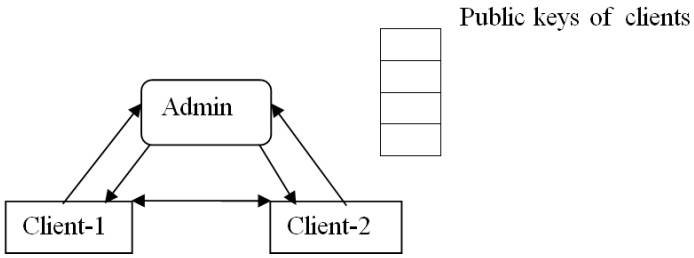

Figure 2: Secure Communication

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.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Implementation of various network exploits and its mitigation techniques using simulators and real devices	**L2**
CO 2	To exploit vulnerabilities in LAN, wireless devices and identify the same using penetration testing	**L4**
CO 3	Exploring the reverse engineering techniques for proper classification of Benign and malicious Desktop applications	**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

24CY731 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 – Optimization Techniques - 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- Behavioral Analysis of Advances Malware such as Ransomwares. Applications of Natural language processing(NLP) in Cyber Security, Attacks on Large Language Models(LLM)- Deep fake technology, Generative AI- Uses, Threat, Simulation and 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**
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/NLP/LLM models in Real time network environments.	**L5**
CO 5	Understand and apply Deep Learning techniques for Network security.	**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

24CY754 WIRELESS NETWORKING AND SECURITY 2-0-3-3

Prerequisite: *CYXXX Internet Protocol lab*

Syllabus:

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, WPA2/3, Security in Bluetooth, 5G security, and IoT wireless protocols.

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	Analyze Threats to Wireless networks and Attacks on 802.11.	**L4**
CO 2	Familiarize with Attacks and mitigation strategy of various Wireless network.	**L4**
CO 3	Explore the security in Bluetooth, 5G security, and IoT wireless protocols	**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

24CY751 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	**L2**
CO 2	Comprehend various error control coding scheme	**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	**L5**
CO 5	Design BCH and RS codes for Channel performance improvement against errors	**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	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

24CY742 STEGANOGRAPHY AND MALWARE ANALYSIS 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, Steg Firewall to prevent malware. Program Analysis: Static-Dynamic- Information Flow-Assembly programming, identify common techniques and approaches for reverse engineering, disassembler, and debugger aided debugging, identifying and defeating anti-disassembly techniques, anti-debugging techniques, code obfuscation. Windows PE file format overview, Windows API & COM overview, Malware persistence mechanisms (Registry by means of service, Trojans, DLL load order hijacking), Rootkits, Privilege elevation mechanisms used by malware, Malware execution (DLL injection, Process replacement, using Hooks and APC), Malware data encoding (common ciphers, custom encodings, Packers YARA rules. Familiarizing with the tools: *Ghidra*, *IDA Pro*, and *GDB Debugger*.

Text Book / References

1. J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st Edition, Cambridge University Press, 2010.
2. C. Collberg and J. Nagra, *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*, Addison-Wesley, 2010.
3. Michael Sikorski and Andrew Honig, *Practical Malware Analysis*, No Starch Press 2012

4. Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sebastien Josse, *Practical Reverse Engineering*, Wiley Publishers, 2014
5. Eldad Eilam, *Reversing: Secrets of Reverse Engineering*, Wiley Publishers, 2005

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding various security issues in multimedia and provide secure measures through steganography	**L3**
CO 2	Familiarizing with different Program analysis techniques	**L4**
CO 3	Exploring various Malware persistence mechanisms and reverse engineering approaches	**L3**
CO 4	Exploring various code obfuscation and Malware data encoding methods	**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
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

24CY741 SECURITY IN CYBER PHYSICAL SYSTEMS 3-0-0-3

Prerequisite: *CYXXX: Network Security*

Syllabus:

Cyber-Physical Systems (CPS), Characteristics, Modules within CPS, Design Process of CPS, Challenges for CPS Software Design, Modeling languages and Tools in CPS, CPS Architecture Layers, Human-Machine Interaction, Power Management, Scalability and Resilience, Edge, and Cloud Computing Integration, Communication Protocols in CPS: MQTT, CoAP, and DDS, Scalability Techniques: Fog Computing, Load Balancing, and Distributed Control, Privacy in CPS, Secure Communication in CPS, Configuring Firewalls, Intrusion Detection and Prevention in CPS, Access Control and Authentication, Security Testing and Evaluation Methods in CPS, Case Studies of CPS Security Breaches and Implications, Emerging Threats: Supply Chain Attacks and Zero-Day Vulnerabilities, Microservices Security, Cloud Services Security, Security Assessment of CPS, Data Analytics for Security in CPS, Code Analysis Tools, Fuzz Testing, Reverse Engineering in CPS, Application of Machine Learning (ML) and Artificial Intelligence (AI) for Anomaly Detection and Threat Prediction in CPS, Formal Methods and Model Checking in CPS Software Verification.

1. Danda B. Rawat, Joel J.P.C. Rodrigues, Ivan Stojmenovic, *Cyber-Physical Systems From Theory to Practice*, CRC Press 2020.
2. Rajeev Alur, *Principles of Cyber-Physical Systems*, MIT Press 2015.
3. Anuradha M. Annaswamy, Pramod P. Khargonekar, Francoise Lamnabhi-Lagarrigue, Sarah K. Spurgeon, *Cyber-Physical-Human Systems: Fundamentals and Applications*, Wiley-IEEE Press 2023.
4. Liu, Yan Zhang, *Cyber Physical Systems Architectures, Protocols and Applications*, CRC Press 2019.
5. Houbing Song, Glenn A. Fink, Sabina Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* Wiley-IEEE Press 2017.

	Course Outcome	Bloom's Taxonomy Level
CO 1	Understanding the System Architecture of the CPS	**L2**
CO 2	Exploring CPS security and privacy	**L3**
CO 3	Familiarization of various vulnerabilities and security testing in CPS	**L4**
CO 4	ML and AI based Threat Prediction in CPS	**L3**
CO 5	Formal Methods and Model checking for software verification	**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	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

24CY732 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	**L2**
CO 2	Design, simulate and synthesis of digital circuits, modules, and systems. Understand the concepts of functions, tasks, user defined primitives, Compiler directives	**L5**

CO 3	Gain the core idea of queues, PLAs, and FSMs. Learn the concepts of FPGAs - blocks inside, their features and use	**L3**
CO 4	FPGA based design realizations	**L5**
CO 5	Design of finite field arithmetic operations, Representative designs with AES, ECC and Hash Algorithms	**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

24CY752 FORMAL METHODS FOR SECURITY 2-0-3-3

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	**L3**

	programs and communication protocols	
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

24CY753 MOBILE SECURITY 2-0-3-3

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

Syllabus

Security of Mobile Networks: Security for Wi-Fi, Telecom, Personal Area Networks, Near Field Communications - Bluetooth, NFC. Security of Mobile Applications: Payments, VoIP, Multimedia. Security of Mobile Platforms: Android, iOS, Windows Phone. Security of Mobile Services: WAP, Mobile HTML, SMS, Location - Android 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, TEE, Reverse Engineering- *Apktool*, *Ghidra*, *Jadx*, code review, Static and Dynamic analysis, runtime instrumentation and smali patching, 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 Deep links, Malware Analysis, *Bouncer*, Privacy Violation, System Call Hardening, ASLR, ROP, Framework Exploits. iOS application and app store, decrypting iOS app, iOS app analysis.

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.
3. Dominic Chell, Tyrone Erasmus, Shaun Colley, and Ollie Whitehouse, *The Mobile Application Hackers Handbook*, Wiley 2015.

	Course Outcome	**Bloom's Taxonomy Level**
CO 1	Android Application development and APK internals	**L6**
CO 2	Understanding the internals of Mobile OS and study the architecture, design and security of mobile computing	**L3**
CO 3	Exploring the Reverse Engineering tools and methodologies	**L4**
CO 4	Familiarize the attacks and Vulnerabilities in apps	**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

24CY761 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 Regulations (GDPR, CCPA, HIPAA, CIS), Cloud - AWS, Azure, GCP. REST API services including load balancing, server authentication and debug handling, Cloud Firewalls, Cloud Peering, - Security Best practices in Cloud: Cloud storage management, Security keys, Customer Managed Encryption keys, Shielded VMs, Encryption and signed URLs, Mitigating DOS stacks in cloud- Hadoop cloud computing framework – HDFS and MapReduce, SPARK, Cloud data processing using Pig and Hive, Amazon EMR for creating Hadoop clusters within AWS, Cloud security Governance, *Prisma*.

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	**L4**
CO 4	Understanding various cloud services and key management problems in cloud storage	**L3**
CO 5	Exploring Hadoop cloud computing framework	**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

24CY762 SPECIAL TOPICS IN CRYPTOGRAPHY 3-0-0-3

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

Syllabus:

Lattice based cryptography - Integer lattices, Hard problems on lattices - Shortest Vector Problem, Closest Vector Problem, Bounded Distance Decoding, Shortest Independent Vector Problem, Learning With Errors, Ring LWE, Short Integer Solution, Ring SIS, Code based cryptography, Hash based cryptography, Homomorphic encryption, BLS signatures, Group signatures, Identity based encryption, Broadcast encryption, Functional encryption, Secure Multi party computation- Visual Cryptography.

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

24CY763 **BLOCKCHAIN TECHNOLOGY** **2-0-3-3**

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

Distributed Ledger Technology (DLT), Blockchain Types, Cryptographic Primitives, Structure of Blockchain, Crypto Wallet , Consensus, Paxos, RAFT, PBFT, PoW, PoS, Bitcoin, Altcoin, Ethereum, MetaMask Wallet, Smart Contracts, Solidity Programming: Structure, Remix IDE, Datatypes, Access Modifiers, Mapping, Web3.js , Hyperledger: Design Principles, Hyperledger Libraries, Tools and DLTs, Hyperledger Fabric: Architecture, Chain code, Deployment of Chain code: Fablo, Hyperledger Bevel, Blockchain Applications, Attacks on Blockchain Consensus and Smart Contracts, Blockchain Forensics, Smart Contract Security

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	**L2**
CO 2	Use of cryptographic primitives in Blockchain technology	**L3**
CO 3	Evaluation of consensus protocols	**L4**
CO 4	Development of smart contracts	**L6**
CO 5	Blockchain and its use cases	**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	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

24CY764 SECURE SYSTEMS ENGINEERING 2-0-3-3

Prerequisite: *CYXXX Concepts in System Security*

Syllabus:

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, Access-controlled and clean environment to build software, Target environment hardening and secure application deployment, Threat Modeling – STRIDE. Risk Assessment - DREAD, Attack trees, Security testing: Common Vulnerabilities and Exploits, CVSS scoring, SAST, DAST, IAST, *SonarQube*, Code smells, Fortify, Fuzzing-AFL. Software security economics - logging/monitoring and operational security aspects, Enhance Detection Engineering with Agile DevSecOps, SOC tech stack, EDR, SOAR, XDR, MDR, Endpoint Security Testing, *Snyk*, Cluster (Kubernetes), Container (Docker) Security, Software Composition Analysis, *Blackduck*, OSS licensing models.

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	Apply Vulnerability analysis into architecture and design process, access-controlled and clean environment to build software, target environment hardening and secure application deployment	**L4**
CO 2	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	**L3**
CO 3	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

24CY765 SPECIAL TOPICS IN CYBER SECURITY 3-0-0-3

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-CMMC, 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

CIR Course - MTech

23HU601	**Career Competency I**	**L-T-P-C: 0-0-3-P/F**

Pre-requisite: An open mind and the urge for self-development, basic English language skills and knowledge of high school level arithmetic.

Course Objectives:

- Help students transit from campus to corporate and enhance their soft skills
- Enable students to understand the importance of goal setting and time management skills
- Support them in developing their problem solving and reasoning skills
- Inspire students to enhance their diction, grammar and verbal reasoning skills

Course Outcomes:

CO1: Soft Skills - To develop positive mindset, communicate professionally, manage time effectively and set personal goals and achieve them.
CO2: Soft Skills - To make formal and informal presentations with self-confidence.
CO3: Aptitude - To analyze, understand and employ the most suitable methods to solve questions on arithmetic and algebra.
CO4: Aptitude - To analyze, understand and apply suitable techniques to solve questions on logical reasoning and data analysis.
C05: Verbal - To infer the meaning of words and use them in the right context. To have a better understanding of the nuances of English grammar and become capable of applying them effectively.

C06: Verbal - To identify the relationship between words using reasoning skills. To understand and analyze arguments and use inductive/deductive reasoning to arrive at conclusions and communicate ideas/perspectives convincingly.

CO-PO Mapping

PO / CO	PO1	PO2	PO3
CO1	2	1	-
CO2	2	1	-
CO3	2	1	-
CO4	2	1	-
CO5	1	2	-
CO6	2	2	-

Syllabus

Soft Skills

Introduction to 'campus to corporate transition':

Communication and listening skills: communication process, barriers to communication, verbal and non-verbal communications, elements of effective communication, listening skills, empathetic listening, role of perception in communication.

Assertiveness skills: the concept, assertiveness and self-esteem, advantages of being assertive, assertiveness and organizational effectiveness.

Self-perception and self-confidence: locus of control (internal v/s external), person perception, social perception, attribution theories-self presentation and impression management, the concept of self and self-confidence, how to develop self-confidence.

Goal setting: the concept, personal values and personal goals, goal setting theory, six areas of goal setting, process of goal setting: SMART goals, how to set personal goals

Time management: the value of time, setting goals/ planning and prioritizing, check the time killing habits, procrastination, tools for time management, rules for time management, strategies for effective time management

Presentation skills: the process of presentation, adult learning principles, preparation and planning, practice, delivery, effective use of voice and body language, effective use of audio visual aids, dos and don'ts of effective presentation

Public speaking-an art, language fluency, the domain expertise (Business GK, Current affairs), self-confidence, the audience, learning principles, body language, energy level and conviction, student presentations in teams of five with debriefing

Verbal

Vocabulary: Familiarize students with the etymology of words, help them realize the relevance of word analysis and enable them to answer synonym and antonym questions. Create an awareness about the frequently misspelt words, commonly confused words and wrong form of words in English.

Grammar: Train students to understand the nuances of English Grammar and thereby enable them to spot grammatical errors and punctuation errors in sentences.

Reasoning: Stress the importance of understanding the relationship between words through analogy questions and learn logical reasoning through syllogism questions. Emphasize the importance of avoiding the gap (assumption) in arguments/ statements/ communication.

Oral Communication Skills: Aid students in using the gift of the gab to improve their debating skills.
Writing Skills: Introduce formal written communication and keep the students informed about the etiquettes of email writing. Make students practise writing emails especially composing job application emails.

Aptitude

Numbers: Types, Power Cycles, Divisibility, Prime, Factors & Multiples, HCF & LCM, Surds, Indices, Square roots, Cube Roots and Simplification.
Percentage: Basics, Profit, Loss & Discount, and Simple & Compound Interest.
Ratio, Proportion & Variation: Basics, Alligations, Mixtures, and Partnership.
Averages: Basics, and Weighted Average.
Time and Work: Basics, Pipes & Cistern, and Work Equivalence.
Time, Speed and Distance: Basics, Average Speed, Relative Speed, Boats & Streams, Races and Circular tracks.
Statistics: Mean, Median, Mode, Range, Variance, Quartile Deviation and Standard Deviation.
Data Interpretation: Tables, Bar Diagrams, Line Graphs, Pie Charts, Caselets, Mixed Varieties, and other forms of data representation.
Equations: Basics, Linear, Quadratic, Equations of Higher Degree and Problems on ages.
Logarithms, Inequalities and Modulus: Basics

References

Soft Skills

Communication and listening skills:

- Andrew J DuRbin , "Applied Psychology: Individual and organizational effectiveness", Pearson-Merril Prentice Hall, 2004
- Michael G Aamodt, "An Applied Approach, 6th edition", Wadsworth Cengage Learning, 2010

Assertiveness skills:

- Robert Bolton, Dorothy Grover Bolton, "People Style at Work..and Beyond: Making Bad Relationships Good and Good", Ridge Associates Inc., 2009
- John Hayes "Interpersonal skills at work", Routledge, 2003
- Nord, W. R., Brief, A. P., Atieh, J. M., & Doherty, E. M., "Meanings of occupational work: A collection of essays (pp. 21- 64)", Lexington, MA: Lexington Books, 1990

Self-perception and self-confidence:

- Mark J Martinko, "Attribution theory: an organizational perspective", St. Lucie, 1995
- Miles Hewstone, "Attribution Theory: Social and Functional Extensions", Blackwell, 1983

Time management:

- Stephen Covey, "The habits of highly effective people", Free press Revised edition, 2004
- Kenneth H Blanchard , "The 25 Best Time Management Tools & Techniques: How to Get More Done Without Driving Yourself Crazy" , Peak Performance Press, 1st edition 2005
- Kenneth H. Blanchard and Spencer Johnson, "The One Minute Manager" , William Morrow, 1984

Verbal

- Erica Meltzer, "The Ultimate Guide to SAT Grammar"
- Green, Sharon, and Ira K. Wolf, "Barron's New GRE", Barron's Educational Series, 2011
- Jeff Kolby, Scott Thornburg & Kathleen Pierce, "Nova's GRE Prep Course"
- Kaplan, "Kaplan New GRE Premier", 2011-2012
- Kaplan's GRE Comprehensive Programme
- Lewis Norman, "Word Power Made Easy", Goyal Publishers, Reprint edition, 1 June 2011

- Manhattan Prep, "GRE Verbal Strategies Effective Strategies Practice from 99th Percentile Instructors"
- Pearson- "A Complete Manual for CAT", 2013
- R.S. Aggarwal, "A Modern Approach to Verbal Reasoning"
- S. Upendran, "Know Your English", Universities Press (India) Limited, 2015
- Sharon Weiner Green, Ira K. Wolf, "Barron's New GRE, 19th edition (Barron's GRE)", 2019
- Wren & Martin, "English Grammar & Composition"
- www.bbc.co.uk/learningenglish
- www.cambridgeenglish.org
- www.englishforeveryone.org
- www.merriam-webster.com

Aptitude

- Arun Sharma, "How to Prepare for Quantitative Aptitude for the CAT Common Admission Test", Tata Mc Graw Hills, 5th Edition , 2012
- Arun Sharma, "How to Prepare for Logical Reasoning for the CAT Common Admission Test", Tata Mc Graw Hills, 2nd Edition, 2014
- Arun Sharma, "How to Prepare for Data Interpretation for the CAT Common Admission Test", Tata Mc Graw Hills, 3nd Edition, 2015
- R.S. Aggarwal, "Quantitative Aptitude For Competitive Examinations", S. Chand Publishing, 2015
- R.S. Aggarwal, "A Modern Approach To Verbal & Non-Verbal Reasoning", S. Chand Publishing, Revised -2015
- Sarvesh Verma, "Quantitative Aptitude-Quantum CAT" , Arihant Publications, 2016
- www.mbatious.com
- www.campusgate.co.in
- www.careerbless.com

Evaluation Pattern

Assessment	**Internal**	**External**
Continuous Assessment (CA)* – Soft Skills	30	-
Continuous Assessment (CA)* – Aptitude	10	25
Continuous Assessment (CA)* – Verbal	10	25
Total	50	50
Pass / Fail		

*CA - Can be **presentations, speaking activities and tests.**

CIR Course - MTech

23HU611	Career Competency II	L-T-P-C: 0-0-3-1

Pre-requisite: Willingness to learn, team spirit, basic English language and communication skills and knowledge of high school level arithmetic.

Course Objectives:

- Help students to understand the importance of interpersonal skills and team work
- Prepare the students for effective group discussions and interviews participation.
- Help students to sharpen their problem solving and reasoning skills
- Empower students to communicate effectively by using the correct diction, grammar and verbal reasoning skills

Course Outcomes:

CO1: Soft Skills - To demonstrate good interpersonal skills, solve problems and effectively participate in group discussions.
CO2: Soft Skills - To write technical resume and perform effectively in interviews.
CO3: Aptitude - To identify, investigate and arrive at appropriate strategies to solve questions on arithmetic by managing time effectively.
CO4: Aptitude - To investigate, understand and use appropriate techniques to solve questions on logical reasoning and data analysis by managing time effectively.
C05: Verbal - To be able to use diction that is more refined and appropriate and to be competent in knowledge of grammar to correct/improve sentences
C06: Verbal - To be able to examine, interpret and investigate passages and to be able to generate ideas, structure them logically and express them in a style that is comprehensible to the audience/recipient.

CO-PO Mapping

PO / CO	PO1	PO2	PO3
CO1	2	1	-
CO2	2	1	-
CO3	2	1	-
CO4	2	1	-
CO5	1	2	-
CO6	2	2	-

Syllabus

Soft Skills

Interpersonal skill: ability to manage conflict, flexibility, empathetic listening, assertiveness, stress management, problem solving, understanding one's own interpersonal needs, role of effective team work in organizations
Group problem solving: the process, the challenges, the skills and knowledge required for the same.

Conflict management: the concept, its impact and importance in personal and professional lives, (activity to identify personal style of conflict management, developing insights that helps in future conflict management situations.)
Team building and working effectively in teams: the concept of groups (teams), different stages of group formation, process of team building, group dynamics, characteristics of effective team, role of leadership in team effectiveness. (Exercise to demonstrate the process of emergence of leadership in a group, debrief and reflection), group discussions.
Interview skills: what is the purpose of a job interview, types of job interviews, how to prepare for an interview, dos and don'ts of interview, One on one mock interview sessions with each student

Verbal

Vocabulary: Help students understand the usage of words in different contexts. Stress the importance of using refined language through idioms and phrasal verbs.
Grammar: Enable students to identify poorly constructed sentences or incorrect sentences and improvise or correct them.
Reasoning: Facilitate the student to tap her/his reasoning skills through critical reasoning questions and logical ordering of sentences.
Reading Comprehension: Enlighten students on the different strategies involved in tackling reading comprehension questions.
Public Speaking Skills: Empower students to overcome glossophobia and speak effectively and confidently before an audience.
Writing Skills: Practice closet tests that assess basic knowledge and skills in usage and mechanics of writing such as punctuation, basic grammar and usage, sentence structure and rhetorical skills such as writing strategy, organization, and style.

Aptitude

Sequence and Series: Basics, AP, GP, HP, and Special Series.
Geometry: 2D, 3D, Coordinate Geometry, and Heights & Distance.
Permutations & Combinations: Basics, Fundamental Counting Principle, Circular Arrangements, and Derangements.
Probability: Basics, Addition & Multiplication Theorems, Conditional Probability and Bayes' Theorem.
Logical Reasoning I: Arrangements, Sequencing, Scheduling, Venn Diagram, Network Diagrams, Binary Logic, and Logical Connectives, Clocks, Calendars, Cubes, Non-Verbal reasoning and Symbol based reasoning.
Logical Reasoning II: Blood Relations, Direction Test, Syllogisms, Series, Odd man out, Coding & Decoding, Cryptarithmetic Problems and Input - Output Reasoning.
Data Sufficiency: Introduction, 5 Options Data Sufficiency and 4 Options Data Sufficiency.
Campus recruitment papers: Discussion of previous year question papers of all major recruiters of Amrita Vishwa Vidyapeetham.
Miscellaneous: Interview Puzzles, Calculation Techniques and Time Management Strategies.

References

Soft Skills

Team Building

- Thomas L.Quick, "Successful team building", AMACOM Div American Mgmt Assn, 1992

- **Brian Cole Miller, "Quick Team-Building Activities for Busy Managers: 50 Exercises That Get Results in Just 15 Minutes", AMACOM; 1 edition, 2003.**
- **Patrick Lencioni, "The Five Dysfunctions of a Team: A Leadership Fable", Jossey-Bass, 1st Edition, 2002**

Verbal

- "GMAT Official Guide" by the Graduate Management Admission Council, 2019
- Arun Sharma, "How to Prepare for Verbal Ability And Reading Comprehension For CAT"
- Joern Meissner, "Turbocharge Your GMAT Sentence Correction Study Guide", 2012
- Kaplan, "Kaplan GMAT 2012 & 13"
- Kaplan, "New GMAT Premier", Kaplan Publishing, U.K., 2013
- Manhattan Prep, "Critical Reasoning 6th Edition GMAT"
- Manhattan Prep, "Sentence Correction 6th Edition GMAT"
- Mike Barrett "SAT Prep Black Book The Most Effective SAT Strategies Ever Published"
- Mike Bryon, "Verbal Reasoning Test Workbook Unbeatable Practice for Verbal Ability, English Usage and Interpretation and Judgement Tests"
- www.bristol.ac.uk/arts/skills/grammar/grammar_tutorial/page_55.htm
- www.campusgate.co.in

Aptitude

- Arun Sharma, "How to Prepare for Quantitative Aptitude for the CAT Common Admission Test", Tata Mc Graw Hills, 5th Edition, 2012
- Arun Sharma, "How to Prepare for Logical Reasoning for the CAT Common Admission Test", Tata Mc Graw Hills, 2nd Edition , 2014
- Arun Sharma, "How to Prepare for Data Interpretation for the CAT Common Admission Test", Tata Mc Graw Hills, 3nd Edition , 2015
- R.S. Aggarwal, "Quantitative Aptitude For Competitive Examinations", S. Chand Publishing , 2015
- R.S. Aggarwal, "A Modern Approach To Verbal & Non-Verbal Reasoning", S. Chand Publishing , Revised -2015
- Sarvesh Verma, "Quantitative Aptitude-Quantum CAT" , Arihant Publications , 2016
- www.mbatious.com
- www.campusgate.co.in
- www.careerbless.com

Evaluation Pattern

Assessment	**Internal**	**External**
Continuous Assessment (CA)* – Soft Skills	30	-
Continuous Assessment (CA)* – Aptitude	10	25
Continuous Assessment (CA)* – Verbal	10	25
Total	50	50

*CA - Can be **presentations, speaking activities and tests.**

22AVP103 Mastery Over Mind (MAOM) 1-0-2 2

1. Course Overview

Master Over the Mind (MAOM) is an Amrita initiative to implement schemes and organise university-wide programs to enhance health and wellbeing of all faculty, staff, and students (UN SDG -3). This program as part of our efforts for sustainable stress reduction gives an introduction to immediate and long-term benefits and equips every attendee to manage stressful emotions and anxiety facilitating inner peace and harmony.

With a meditation technique offered by Amrita Chancellor and world-renowned humanitarian and spiritual leader, Sri Mata Amritanandamayi Devi (Amma), this course has been planned to be offered to all students of all campuses of AMRITA, starting off with all first years, wherein one hour per week is completely dedicated for guided practical meditation session and one hour on the theory aspects of MAOM. The theory section comprises lecture hours within a structured syllabus and will include invited guest lecture series from eminent personalities from diverse fields of excellence. This course will enhance the understanding of experiential learning based on university's mission: "Education for Life along with Education for Living", and is aimed to allow learners to realize and rediscover the infinite potential of one's true Being and the fulfilment of life's goals.

2. Course Syllabus

Unit 1 (4 hours)

Causes of Stress: The problem of not being relaxed. Need for meditation -basics of stress management at home and workplace. Traditions and Culture. Principles of meditation– promote a sense of control and autonomy in the Universal Human Value System. Different stages of Meditation. Various Meditation Models. Various practices of Meditation techniques in different schools of philosophy and Indian Knowledge System.

Unit 2 (4 hours)

Improving work and study performance. Meditation in daily life. Cultivating compassion and good mental health with an attitude of openness and acceptance. Research and Science of Meditation: Significance of practising meditation and perspectives from diverse fields like science, medicine, technology. philosophy, culture, arts, management, sports, economics, healthcare, environment etc. The role of meditation for stress and anxiety reduction in one's life with insights based on recent cutting-edge technology. The effect of practicing meditation for the wholesome wellbeing of an individual.

Unit 3 (4 hours)

Communications: principles of conscious communication. Relationships and empathy: meditative approach in managing and maintaining better relationships in life during the interactions in the world, role of MAOM in developing compassion, empathy and responsibility, instilling interest, and orientation to humanitarian projects as a key to harness intelligence and compassion in youth. Methodologies to evaluate effective awareness and relaxation gained from meditation. Evaluating the global transformation through meditation by instilling human values which leads to service learning and compassion driven research.

TEXT BOOKS:

1.Mata Amritanandamayi Devi, "Cultivating Strength and vitality," published by Mata Amritanandamayi Math, Dec 2019

2.Swami Amritaswarupananda Puri ,"The Color of Rainbow " published by MAM, Amritapuri.

REFERENCES:

1.Craig Groeschel, "Winning the War in Your Mind: Change Your Thinking, Change Your Life" Zondervan Publishers, February 2019
2.R Nagarathna et al, "New Perspectives in Stress Management "Swami Vivekananda Yoga Prakashana publications, Jan 1986
3. Swami Amritaswarupananda Puri "Awaken Children Vol 1, 5 and 7 - Dialogues with Amma on Meditation", August 2019
4. Swami Amritaswarupananda Puri "From Amma's Heart - Amma's answer to questions raised during world tours" March 2018
5. Secret of Inner Peace- Swami Ramakrishnananda Puri, Amrita Books, Jan 2018.
6. Mata Amritanandamayi Devi "Compassion :The only way to Peace:Paris Speech", MA Center, April 2016.
7. Mata Amritanandamayi Devi "Understanding and collaboration between Religions", MA Center, April 2016.
8. Mata Amritanandamayi Devi "Awakening of Universal Motherhood: Geneva Speech" M A center, April 2016.

3. Evaluation and Grading

Internal			**External**	**Total**
Components	*Weightage*		Practical (attendance and class participation) 60%	100%
Quizzes(based on the reading material)	20%	40%		
Assignments (Based on webinars and lecture series)	20%			

4. Course Outcomes (CO)

CO1: Relate to the causes of stress in one's life.
CO2: Experiment with a range of relaxation techniques
CO3: Model a meditative approach to work, study, and life.
CO4: Develop appropriate practice of MA-OM technique that is effective in one's life
CO5: Inculcate a higher level of awareness and focus.
CO6: Evaluate the impact of a meditation technique

***Program Outcomes (PO)** (As given by NBA and ABET)
PO1: Engineering Knowledge
PO2: Problem Analysis
PO3: Design/Development of Solutions
PO4: Conduct Investigations of complex problems
PO5: Modern tools usage
PO6: Engineer and Society
PO7: Environment and Sustainability
PO8: Ethics
PO9: Individual & Team work
PO10: Communication
PO11: Project management & Finance
PO12: Lifelong learning

CO – PO Affinity Map

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PS01	PSO2	PSO3
CO 1	3	3	3	2		-	2	3	-	3	-	3	-	-	-
CO 2	3	3	3	2	2	_	2	3	3	3	-	3	-	-	-
CO 3	3	3	2	2	2	2	2	3	3	3	-	3	-	-	-
CO 4	3	3	3	2	-	2	3	3	3	3	-	3	-	-	-
CO 5	3	2	2	2	-	2	-	3	2	2	-	2	-	-	-
CO 6	3	2	2	2	3	2	_	3	2	2	-	2	-	-	-