M. TECH - CYBER SECURITY

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

2026

Cyber Security is a very fast-moving field. A program in security that aims to be at the forefront has to necessarily have a companion-advanced program that has a good balance between theoretical and practical aspects, analytical methods, 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 the 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 can also 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, and 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 to 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
26MA601	FC	Mathematical Foundations for Cyber Security	2 0 0	2
26CY602	SC	Network Security	3 0 0	3
26CY603	FC	Cryptography	3 0 3	4
26CY681	SC	Internet Protocol lab	0 0 6	2
26CY604	SC	Web Application Security	3 0 3	4
26CY605	SC	Secure Coding	2 0 3	3
26RM602	P	Research Methodology	2 0 0	2
25AVP501	HU	Mastery Over Mind	1 0 2	2
22ADM501	HU	Glimpses of Indian Culture	2 0 1	P/F
23HU601	HU	Career Competency I	0 0 3	P/F
				Credits 22

Second Semester

Course Code	Type	Course	L T P	C
26CY611	SC	Cyber Forensics	2 0 3	3
26CY612	SC	Applied Cryptography	3 0 3	4
26CY613	FC	Concepts in System Security	2 0 3	3
	E	Elective I		3
	E	Elective II		3
26CY682	SC	Cyber Security Lab	0 0 9	3
26CUL500	HU	Integrated Amrita Meditation Technique	0 0 2	1
23HU611	HU	Career Competency II	0 0 3	1
				Credits 21

Third Semester

Course Code	Type	Course	L T P	C
	E	Elective III		3
	E	Elective IV		3
26CY798	P	Dissertation I		10
				Credits 16

Fourth Semester

Course Code	Type	Course	L T P	C
26CY799	P	Dissertation II		15
				Credits 15

Total Credits: 74

List of Courses
Foundation Core

Course Code	Course	L T P	C
26MA601	Mathematical Foundations for Cyber Security	2 0 0	2
26CY613	Concepts in System Security	2 0 3	3
26CY603	Cryptography	3 0 3	4

Subject Core

Course Code	Course	L T P	C
26CY611	Cyber Forensics	2 0 3	3
26CY612	Applied Cryptography	3 0 3	4
26CY602	Network Security	3 0 0	3
26CY604	Web Application Security	3 0 3	4
26CY605	Secure Coding	2 0 3	3

Laboratory

Course Code	Course	L T P	C
26CY681	Internet Protocol Lab	0 0 6	2
26CY682	Cyber Security Lab	0 0 9	3

Electives

Course Code	Course	L T P	C
	Elective I		
26CY731	AI for Cyber Security Applications	2 0 3	3
26CY732	Cryptographic Hardware and Embedded Systems	2 0 3	3
	Elective II		
26CY741	Security of Cyber Physical Systems	3 0 0	3
26CY742	Steganography and Malware Analysis	2 0 3	3
	Elective III		
26CY751	Coding and Information Theory	3 0 0	3
26CY752	Formal Methods for Security	2 0 3	3
26CY753	Mobile Security	2 0 3	3
26CY754	Wireless Networking and Security	2 0 3	3
26CY755	Security in AI	2 0 3	3
	Elective IV		
26CY761	Security in Cloud Computing	2 0 3	3
26CY762	Special Topics in Cryptography	3 0 0	3
26CY763	Blockchain Technology	2 0 3	3
26CY764	Secure Systems Engineering	2 0 3	3
26CY765	Special Topics in Cyber Security	3 0 0	3

Project

Course Code	Courses	L T P	Cr
26CY798	Dissertation I		10
26CY799	Dissertation II		15

26MA601 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 2-0-0-2

Prerequisites: *Basics of Set Theory*

Syllabus:

Elementary Number Theory, Congruence, Quadratic Residues, Primitive roots, Algorithms for primality testing, Integer Factorization, and Discrete Logarithm. Algebraic Structures - Groups, Vector space, Subspace, Inner product spaces, Orthogonalization, Diagonalization.

Text Book / References

1. S.Y. Yan, *Number Theory for Computing*, 2nd Edition, Springer, Berlin, 2002.
2. Rosen, Kenneth H., Elementary Number Theory and Its Applications, 6th Edition, Pearson Education, New Delhi, 2011.
3. Shoup, Victor, A Computational Introduction to Number Theory and Algebra, 2nd Edition, Cambridge University Press, Cambridge, 2009.
4. Gallian, Joseph A., Contemporary Abstract Algebra, 10th Edition, Cengage Learning, Boston, MA, 2023.
5. Strang, Gilbert, Introduction to Linear Algebra, 6th Edition, Wellesley-Cambridge Press, Wellesley, Massachusetts, 2023.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Apply concepts of number theory, congruences, quadratic residues, and primitive roots.	**L4**
CO 2	Analyze algorithms for primality testing, integer factorization, and discrete logarithms.	**L4**
CO 3	Apply algebraic structures, vector spaces, inner product spaces, orthogonalization, and diagonalization.	**L3**

CO-PO Mapping (1-Low, 2-Medium, 3-High)													
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	3	2	-	-	2	2	-	-	-	-	2	3	1
CO 2	3	3	2	2	2	2	-	-	-	-	2	3	3
CO 3	2	2	-	-	2	2	-	1	-	-	2	2	1

26CY602 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; Zero Trust Network Architecture (ZTNA), 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.
5. Gilman, E., & Barth, D. (2017). *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media.

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

CO-PO Mapping (1-Low, 2-Medium, 3-High)													
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	2	-	-	1	2	-	3	3	3
CO 2	2	2	2	2	2	-	-	1	2	-	3	3	3
CO 3	2	2	2	2	2	-	-	1	2	-	3	3	3
CO 4	2	2	2	2	2	-	-	1	2	-	3	3	3
CO 5	2	2	2	2	2	-	-	1	2	-	3	3	3

Prerequisites:
Elementary Number Theory, Modular Arithmetic, Groups, Rings, Fields, Probability Basics.

Syllabus:
Foundations of Cryptography: Security goals and attacks, Computational security, Perfect secrecy, One-time pad and its limitations, Pseudorandom generators, Stream ciphers, Linear feedback shift registers (LFSRs), Cryptanalysis of linear generators.
Symmetric-Key Cryptography: 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. Authenticated Encryption-Authenticated encryption ciphers from generic composition,
Public key encryption: RSA, 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, Homomorphic encryption, Order preserving encryption, searchable encryption.

Text Book / References

1. Douglas Robert Stinson, Maura Paterson. Cryptography: Theory and Practice (Textbooks in Mathematics). Fourth Edition. Chapman and Hall/CRC;2018.
2. Hoffstein, Jeffrey, Pipher, Jill, and Silverman, Joseph H., An Introduction to Mathematical Cryptography, 2nd Edition, Springer, New York, 2014.
3. Paar, Christof and Pelzl, Jan, Understanding Cryptography: A Textbook for Students and Practitioners, 2nd Edition, Springer, Berlin, 2024.
4. Boneh, Dan and Shoup, Victor, A Graduate Course in Applied Cryptography, Version 0.6, 2023.
5. Wade Trappe, Lawrence C Washington, Introduction to Cryptography with Coding Theory, Pearson, 2006
6. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography: Theory and Practice*, Pearson Education India, 2009.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Apply the principles of symmetric-key cryptography, including stream ciphers, block ciphers, hash functions, and message authentication mechanisms	**L3**
CO 2	Analyze public-key cryptographic schemes, key exchange protocols, and digital signature algorithms used in secure communication systems.	**L4**
CO 3	Evaluate advanced cryptographic techniques and their applications in cyber security, including authenticated encryption, elliptic curve cryptography, homomorphic encryption, and searchable encryption.	**L4**

CO-PO Mapping (3-High, 2-Medium, 1-Low)

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

26CY681 INTERNET PROTOCOL LAB 0-0-6-2

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

Syllabus:

Network diagnostics and troubleshooting using Ping, Traceroute, Netstat/SS, ARP, Nslookup/Dig, Netcat (nc), IP configuration, and routing utilities. Packet capture and traffic monitoring using Wireshark. Protocol analysis and visualization of Ethernet, ARP, IPv4, IPv6, ICMP, TCP, UDP, DHCP, DNS, HTTP, HTTPS/TLS, SMTP, FTP, and IEEE 802.11 Wi Fi protocols. Traffic filtering, packet inspection, throughput analysis, and network performance measurement using Wireshark and iPerf/iPerf3. Network threat hunting and traffic forensic analysis using PCAP files for identification of malware communication, network attacks, and Indicators of Compromise (IoCs). Network topology design, implementation, and simulation using Cisco Packet Tracer. Configuration and analysis of routing protocols, including Static Routing, RIP, OSPF, and BGP. Configuration and analysis of switched and wireless networks using VLANs, Inter-VLAN Routing, WLANs, and wireless security mechanisms. Introduction to Software Defined Networking (SDN) concepts using Mininet/OpenFlow. Network emulation and traffic control using Linux Traffic Control (tc), including bandwidth management, latency, packet loss, and traffic shaping. Analysis of secure Internet protocols and services, including TLS/SSL, DNSSEC, VPN, and tunneling concepts. Socket programming using Python for TCP sockets, UDP sockets, client-server applications, and multi-client communication. Secure network programming using classical cryptography, symmetric key cryptography, RSA, Diffie-Hellman key exchange, and TLS-based secure communication. Familiarization with secure network design principles, protocol security analysis, and performance evaluation of Internet protocols.

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(CO)		Bloom's Taxonomy Level
CO 1	Analyze Internet protocols, network services, and packet-level communication using network diagnostic, monitoring, and traffic analysis tools.	**L4**
CO 2	Illustrate data transfer, congestion control, and flow handling mechanisms of transport layer protocols through network performance analysis and emulation.	**L3**
CO 3	Understand the working principles of routing mechanisms and analyze routing protocols for determining optimal network paths.	**L4**
CO 4	Understand switched, wireless, and software-defined networking concepts, secure Internet protocols, and network security	**L2**

	mechanisms.	
CO 5	Develop network applications and secure communication systems using socket programming and cryptographic techniques.	**L3**

CO-PO Mapping (3-High, 2-Medium, 1-Low)													
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	3	3	1	1	-	2	1	2	3	2
CO 2	2	3	2	3	3	1	1	-	2	1	2	3	2
CO 3	2	3	3	3	2	1	1	-	2	1	2	3	2
CO 4	3	2	3	3	2	1	1	-	2	1	2	3	2
CO 5	3	3	3	3	3	2	1	-	2	1	2	3	2

26CY604 WEB APPLICATION SECURITY 3-0-3-4

Prerequisites: *Basics of Web development* (*HTML, CSS, JavaScript, server-side scripting language*

Syllabus:

Web application development basics – Client-side technologies – Server-side technologies– Authentication and access control – Session management techniques – OWASP Top 10 flaws – Web application technologies – vulnerabilities.

Server-side attacks – SQL injection – OS command injection – Directory traversal – Business logic vulnerabilities – Access Control Vulnerabilities and Privilege Escalation –XML external entity (XXE) injection – Server-side request forgery (SSRF) – Web cache deception – API testing.

Client-side attacks – Cross-site Scripting (XSS) – Cross-site Request Forgery (CSRF) – Cross-origin resource sharing (CORS) – Clickjacking – Web Cache Poisoning – DOM-based vulnerabilities.

Web 3.0 architecture and security – Web sockets security – Web LLM attacks – HTTP request smuggling – Web Cache Poisoning – JWT attacks.

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(CO)		**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 techniques to prevent security vulnerabilities.	**L3**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY605 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, AI-assisted secure coding.

Textbook / References

1. Goodrich MT, Tamassia R, Goldwasser MH. Data Structures and Algorithms in Java. Sixth edition, John Wiley & Sons Ltd; 2014.
2. Robert C. Seacord, *The CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems*, 2nd Edition, Pearson Education, 2016.
3. CERT C Coding Standard. https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard.

Course Outcome (CO)		Bloom's Taxonomy Level
CO 1	Identify and mitigate the vulnerabilities based on string manipulation errors.	**L3**
CO 2	Identify and mitigate the vulnerabilities due to dynamic memory management errors.	**L4**
CO 3	Identify and mitigate the vulnerabilities based on integer operations and errors in formatted output	**L3**
CO 4	Identify and mitigate the vulnerabilities based on race conditions	**L4**

CO-PO Mapping (3-High, 2-Medium, 1-Low)													
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

26RM602 **Research Methodology** **2 0 0 2**

Prerequisites:

1. *Basic academic writing skills*
2. *Fundamental understanding of scientific and technical subjects*

Syllabus:

Unit I – Foundations of Research and Scientific Inquiry Meaning, objectives, and types of research. Research process and lifecycle. Problem definition and formulation. Research objectives and research questions. Research design and research approaches. Understanding theory in research. Exploratory vs. confirmatory research. Experimental vs. theoretical research. Importance of reasoning in research. Critical thinking in scientific inquiry. Understanding novelty and research gaps.

Unit II – Literature Review and Research Communication Conducting a literature review. Referencing and citation practices. Information sources and information retrieval. Role of libraries in information retrieval. Tools for identifying literature. Indexing and abstracting services. Citation indexes and citation metrics. Navigating research databases. Systematic literature review methods. Preparation and structure of research papers. Writing abstracts, introductions, methodology, results, discussions, and conclusions. Tables, illustrations, and graphical representations. Documentation standards and manuscript preparation, PRISMA methodology

Unit III – Experimental Design, Data Analysis, and Visualization Understanding modeling and simulation. Experimental research and scientific hypothesis testing. Development and writing of hypotheses. Measurement systems analysis. Validity and reliability of experiments. Statistical design of experiments. Field experiments. Data and variable types and classification. Data collection methods. Sampling, observation, and surveys. Numerical and graphical data analysis. Inferential statistics and interpretation of results. Data visualization techniques including charting and graphing.

Unit IV – Artificial Intelligence in Research Methodology Evolution of AI in scientific research workflows. AI as a cognitive assistant in research. Human– AI collaboration in scholarly inquiry. AI-assisted academic search and semantic retrieval. AI tools for identifying research gaps and novelty. Citation network analysis using AI tools. AI support in exploratory data analysis and visualization. Machine learning concepts relevant to research methodology. AI-assisted pattern recognition and hypothesis refinement. Role of AI in qualitative data analysis including coding and theme extraction. Risks of hallucination and fabricated citations in generative AI. Limitations of AI in scientific argumentation. Distinction between editing support and authorship. Bias detection in datasets using AI tools. Ethical limits of AI-driven inference. Human validation of AI-generated analytical results.

Unit V – Ethics, Intellectual Property, and Responsible Research Research integrity and responsible conduct of research. Research ethics and scientific misconduct. 22 Forms of scientific misconduct. Plagiarism and unscientific practices in thesis work. Ethics in science and responsible conduct of research. Reproducibility and transparency in research. Intellectual Property Rights (IPR): patents, copyrights, trademarks, industrial designs, and geographical indications. Ethical risks of AI-generated research outputs. Bias, fairness, and representativeness in AI models. AI hallucination and misinformation risks. AI transparency and accountability. Reproducibility and explainability in AI-

supported research. Ownership of AI-generated content. AI and Intellectual Property Rights. Regulatory and policy perspectives on AI in academia.

Text Books / References

1. Bordens, K. S. and Abbott, B. B., Research Design and Methods – A Process Approach, 8th Edition, McGraw-Hill, 2011.
2. Kothari, C. R., Research Methodology – Methods and Techniques, 2nd Edition, New Age International Publishers.
3. Creswell, J. W., Research Design, Sage Publications.
4. Davis, M., Davis K., and Dunagan M., Scientific Papers and Presentations, 3rd Edition, Elsevier Inc.
5. Michael P. Marder, Research Methods for Science, Cambridge University Press, 2011.
6. T. Ramappa, Intellectual Property Rights Under WTO, S. Chand, 2008.
7. Robert P. Merges, Peter S. Menell, and Mark A. Lemley, Intellectual Property in the New Technological Age, Aspen Law & Business, 6th Edition, 2012.
8. Russell, Stuart, and Peter Norvig. "Artificial Intelligence: A Modern Approach, UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021.
9. Floridi, Luciano, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, Oxford University Press, 2023.
10. OECD, AI, Data Governance and Privacy, OECD Publishing, 2024.
11. Kitchenham, B., and Charters, S., Guidelines for Performing Systematic Literature Reviews in Software Engineering.
12. van Eck, N.J., and Waltman, L., Citation-based Clustering of Publications Using CitNetExplorer and VOSviewer, Scientometrics, 2017.
13. Elsevier, The Use of Generative AI and AI-assisted Technologies in Writing, 2025.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Explain research methodologies and formulate research problems.	**L2**
CO 2	Conduct literature reviews and prepare scholarly research documents using appropriate tools and practices.	**L3**
CO 3	Design, analyse, and interpret research studies using appropriate analytical techniques.	**L4**
CO 4	Apply research ethics, intellectual property principles, and responsible AI practices in research.	**L3**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PSO1	PSO2	PSO3
CO1	1	2	-	1	1	2	-	-	-	-	1	2	2
CO2	-	2	-	-	2	3	3	-	3	-	-	2	2
CO3	2	3	2	2	2	3	2	-	1	-	1	3	3

CO4	-	1	-	1	1	2	-	-	1	3	3	1	1

26CY611 CYBER FORENSICS 2-0-3-3

Prerequisites: *26CY602 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), AI-Assisted Digital Forensics, Generative AI and Deepfake Forensics

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, *Cybersecurity: 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 Beginner's Guide*, McGraw-Hill Education, 2013.
6. Bill Nelson, Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations*, 4th Edition, 2014.
7. Omar, M., & Zangana, H. M. (Eds.). (2024). *Digital Forensics in the Age of AI*. IGI Global.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Exploring the fundamentals of forensics for Windows and Unix Systems.	**L3**
CO 2	Exploring the ideas of the digital forensics framework and laws	**L3**
CO 3	Familiarizing the ideas of network systems and Web Application Forensics.	**L4**
CO 4	Exploring the ideas of Email and Database forensics	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY612 APPLIED CRYPTOGRAPHY 3-0-3-4

Prerequisites: *26CY603 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. Boyd, Colin, Anish Mathuria, and Douglas Stebila. Introduction to Authentication and Key Establishment. Protocols for Authentication and Key Establishment. Springer, Berlin, Heidelberg; 2020
1. Boneh, Dan, and Victor Shoup. A graduate course in applied cryptography. Draft 0.5; 2020
2. A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1996.
3. J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of computer security*, Springer, 2003.
4. Abhijit Das and Veni Madhavan C. E., *Public-Key Cryptography, Theory and Practice*, Pearson Education, 2009.
5. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Apply identification, authentication, and password-based protocols for secure user access and communication.	**L4**
CO 2	Analyze key exchange and authenticated key exchange protocols, including their security properties and common attacks.	**L4**
CO 3	Evaluate advanced authentication and key management mechanisms such as zero-knowledge protocols, conference key protocols, key broadcasting protocols, and federated identity systems.	**L4**

CO-PO Mapping (3-High, 2-Medium, 1-Low)													
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	3	2	2	1	3	-	-	-	-	1	3	3	2
CO 2	3	3	3	3	2	2	-	-	-	1	2	3	3
CO 3	2	3	2	3	2	3	1	-	1	1	2	3	3

26CY613 CONCEPTS IN SYSTEM SECURITY 2-0-3-3

Prerequisites:
Basic knowledge of concurrency and access control. Practical experience in installation, monitoring, and troubleshooting of operating systems (Windows and Linux)

Syllabus:
Program- processes- Binaries - Libraries- 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 - Concurrency control - Operating System Security Architecture - User Mode and Kernel Mode – Process Isolation – File System Security – Access Control Models (DAC, MAC, RBAC, ABAC) – Authentication and Credential Management – Linux Security Modules – SELinux, CVE/CWE ecosystems, Sandboxing- Virtualization techniques for security - Trusted computing – TEE, Zero Trust Security, Distributed systems security, and Windows vs. Linux security comparison.

Text Book / References

1. Wenliang Du, *Computer Security – A hands-on Approach*, First Edition, CreateSpace Independent Pub, 2017
2. T. Jaeger, *Operating System Security*, Vol. 1 of Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers, 2008.
3. W. Mauerer, *Professional Linux Kernel Architecture*, John Wiley and Sons, New York, 2008.
4. R Anderson, *Security engineering*, John Wiley & Sons, 2008.
5. Matt Bishop, *Computer Security: Art and Science*, Vol. 2, Addison-Wesley, 2012.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Understand process management, process memory organization, SetUID programs, environment variables, and their associated attacks.	**L2**
CO 2	Analyze operating system exploitation techniques and corresponding security defense mechanisms.	**L3**
CO 3	Understand and apply access control models and authentication mechanisms to secure operating systems and computing systems.	**L4**
CO 4	Apply virtualization and trusted computing techniques to enhance system security.	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY682 CYBER SECURITY LAB 0-0-9-3

Prerequisite: *Basic network troubleshooting, OSI layers, Basic usage of Linux utilities and networking tools.*

Syllabus:

Objectives

1. To familiarize with Linux tools and networking utilities.
2. To configure centralized log monitoring using Splunk Enterprise.
3. To perform LAN-based attacks and analyze the generated logs and traffic.
4. To perform web-based attacks and analyze the generated logs and traffic.
5. To perform network scanning using Nmap with different scanning techniques.
6. To perform scripting and enumeration using Nmap NSE scripts.
7. To perform vulnerability assessment using Nessus.
8. To analyze attacks, scans, and network traffic using Wireshark and Splunk Enterprise.
9. To configure and monitor systems using Wazuh.
10. To exploit Windows and Linux vulnerabilities using Metasploit and Meterpreter.
11. To perform wireless network attacks and wireless traffic analysis.
12. To understand Active Directory architecture and perform Active Directory security analysis.

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

Experiment No. 1: Introduction to Linux Tools

Familiarize with the Linux operating system and commonly used networking and security tools.

1. Practice basic Linux commands for file handling and system administration.
2. Familiarize with networking tools such as: ping, traceroute, netstat, ss, tcpdump, curl, wget
3. Practice process monitoring and service management commands.
4. Familiarize with file permissions and user management.
5. Practice basic shell scripting and package management.

Experiment No. 2: Centralized Log Monitoring using Splunk

Install and configure Splunk Enterprise in a centralized server environment.

1. Install Splunk server in a dedicated machine.
2. Install Splunk Universal Forwarder in all client systems.
3. Configure log forwarding from Linux and Windows systems.
4. Capture and analyze: System logs, Authentication logs, Firewall logs, Web server logs.
5. Familiarize with: Indexing, Searching, Dashboards, Alerts, SPL Queries.

Experiment No. 3: LAN-Based Attacks and Analysis

Perform LAN-based attacks and analyze the generated logs and network traffic.

1. Perform ARP spoofing and ARP cache poisoning attacks.
2. Perform DNS spoofing attacks.
3. Perform MAC flooding attacks.
4. Perform Man-in-the-Middle (MITM) attacks.
5. Observe the ARP table and CAM table before and after the attacks.
6. Capture packets using Wireshark.
7. Forward attack logs to Splunk Enterprise and analyze the events. Tools used: Ettercap, Bettercap, Wireshark.

Experiment No. 4: Web-Based Attacks and Analysis

Perform Web application attacks and analyze the logs and captured traffic.

1. Perform SQL Injection attacks.
2. Perform Cross-Site Scripting (XSS) attacks.
3. Perform Brute force login attacks.
4. Perform Directory Traversal attacks.
5. Capture HTTP/HTTPS traffic using Wireshark.
6. Capture web server logs and analyze them using Splunk Enterprise. Tools used: Burp Suite and OWASP ZAP

Experiment No. 5: Network Scanning using Nmap

Use Nmap to perform different types of network scanning.

1. Perform a Ping Sweep to identify live hosts.
2. Perform TCP Connect Scan.
3. Perform SYN Scan.
4. Perform FIN Scan.
5. Perform Xmas Scan.
6. Perform UDP Scan.
7. Perform OS Fingerprinting.
8. Perform Service Version Detection.
9. Analyze the generated traffic using Wireshark.
10. Capture and analyze scan logs using Splunk Enterprise.

Experiment No. 6: Nmap Scripting and Enumeration

Perform enumeration and vulnerability detection using Nmap NSE scripts.

1. Perform SMB enumeration.
2. Perform HTTP enumeration.
3. Perform FTP anonymous login detection.
4. Perform SSH brute force testing.
5. Perform vulnerability scanning using NSE scripts.
6. Analyze the generated logs and packets using: Splunk Enterprise, Wireshark

Experiment No. 7: Vulnerability Assessment using Nessus

Perform vulnerability assessment using Nessus.

1. Install and configure Nessus.
2. Perform Host Discovery scan.
3. Perform Basic Network Scan.
4. Perform Web Vulnerability Scan.
5. Analyze the identified vulnerabilities.
6. Generate vulnerability reports.
7. Correlate the scan logs using Splunk Enterprise.

Experiment No. 8: Traffic and Log Analysis using Splunk and Wireshark

Analyze all the attacks and scans performed in previous experiments.

1. Capture packets using Wireshark.
2. Correlate logs using Splunk Enterprise.

3. Analyze: Attack signatures, Network anomalies, Suspicious traffic, and authentication failures.
4. Create dashboards and alerts in Splunk.

Experiment No. 9: Setup and Configuration of Wazuh

Install and configure Wazuh for monitoring and threat detection.

1. Install Wazuh Manager.
2. Configure Wazuh agents in Linux and Windows systems.
3. Configure log monitoring and alerting.
4. Familiarize with: File Integrity Monitoring, Rootkit Detection, Vulnerability Detection, Active Response
5. Analyze alerts generated by Wazuh.

Experiment No. 10: LAN and Web Attack Detection using Wazuh

Perform LAN and web-based attacks again and monitor the generated alerts using Wazuh.

1. Perform LAN-based attacks.
2. Perform Web-based attacks.
3. Monitor generated alerts in the Wazuh dashboard.
4. Analyze attack logs and rule matching.
5. Compare the detection capability of Splunk and Wazuh.

Experiment No. 11: Exploiting Vulnerabilities using Metasploit

Use Metasploit and Meterpreter to exploit Windows and Linux vulnerabilities.

1. Set up vulnerable Windows and Linux virtual machines.
2. Perform vulnerability scanning.
3. Exploit vulnerabilities using Metasploit modules.
4. Establish Meterpreter sessions.
5. Perform: Privilege Escalation, File Access, Command Execution.
6. Capture logs and analyze the attacks using Splunk Enterprise, Wazuh, and Wireshark.

Experiment No. 12: Wireless Security Lab

Perform wireless network attacks and wireless traffic analysis.

1. Perform wireless network reconnaissance.
2. Capture WPA/WPA2 handshake packets.
3. Perform deauthentication attacks.
4. Perform wireless packet sniffing.
5. Analyze wireless traffic using Wireshark.
6. Perform wireless auditing using Aircrack-ng and Kismet.

Experiment No. 13: Active Directory Security Lab

Understand Active Directory architecture and perform Active Directory security analysis.

1. Set up Windows Server as a Domain Controller.
2. Configure users, groups, and policies.

3. Perform Active Directory enumeration.
4. Analyze authentication logs and Kerberos events.
5. Perform privilege escalation and lateral movement analysis.
6. Monitor and analyze Active Directory logs using: Splunk Enterprise, Wazuh

Text Book / References

1. The Web Application Hacker's Handbook, Dafydd Stuttard and Marcus Pinto, Wiley Publishing, 2nd Edition.
2. Nmap Network Scanning, Gordon "Fyodor" Lyon, Insecure.Org LLC.
3. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, No Starch Press.
4. Practical Malware Analysis, Michael Sikorski and Andrew Honig, No Starch Press.
5. The Practice of Network Security Monitoring, Richard Bejtlich, No Starch Press.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Analyze network traffic, system logs, and security events using Linux tools, Wireshark, Splunk Enterprise, and Wazuh.	**L2**
CO 2	Perform network reconnaissance, enumeration, and vulnerability assessment using Nmap, NSE scripts, and Nessus.	**L4**
CO 3	Implement and analyze network, web application, and wireless attacks in controlled environments and evaluate their security implications.	**L4**
CO 4	Exploit and investigate Windows, Linux, and Active Directory security vulnerabilities using penetration testing and security monitoring frameworks.	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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	3	3	2	-	1	-	-	3	3	3
CO 2	2	3	3	3	3	2	-	1	-	-	3	3	3
CO 3	3	3	3	3	3	2	-	1	-	-	3	3	3
CO 4	3	3	3	3	3	2	-	1	-	-	3	3	3

26CY731 **AI for Cyber Security Applications** **2-0-3-3**

Prerequisites: *Statistics and Probability*
Syllabus

Foundations of AI for Cyber Security: Introduction to Artificial Intelligence, Evolution of AI, AI vs. Machine Learning vs. Deep Learning vs. Generative AI, Types of Learning – Supervised, Unsupervised, Semi-supervised and Reinforcement Learning, Neural Networks and Decision Trees. Cybersecurity Foundations: CIA Triad, Threat Actors and Attack Vectors. Data Collection and Preprocessing, Feature Engineering, Feature Selection, Dimensionality Reduction, Model Training and Validation, Overfitting and Underfitting, Performance Evaluation Metrics. Python for Security Analytics, Security Datasets, Log Collection and Preprocessing Pipelines. **Machine Learning and Deep Learning for Threat Detection:** Classification, Clustering and Dimensionality Reduction Techniques, Perceptron, Multi-Layer Perceptron, Backpropagation, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, Variational Autoencoders, Generative Adversarial Networks (GANs), Large Language Models (Architectural Overview), AI-based Anomaly Detection, Applications of Machine Learning and Deep Learning in Cyber Security. **AI-Driven Cyber Security Operations:** AI System Architectures and Security Applications, Foundation Models, Retrieval-Augmented Generation (RAG), Agentic AI, AI for Threat Detection and Prevention, Malware Analysis and Classification, Vulnerability Assessment and Prioritization, AI-assisted Penetration Testing and Red Teaming, Phishing and Spam Detection, Deepfake Detection and Media Forensics, Natural Language Processing for Threat Intelligence, Security Information and Event Management (SIEM), AI-powered Security Operations Centres (SOC), Threat Hunting, Real-time Threat Detection, Explainable AI (XAI), Continuous Authentication, AI-assisted Incident Response and Forensics, AI-based Cyber Risk Assessment, Secure AI Lifecycle, MLOps and SecOps Integration, Threat Modelling for AI Systems, AI Risk Management, Adversarial Machine Learning, LLM and Prompt Security Risks, Emerging Trends and Applications in AI-driven Cyber Security.

Textbook(s):

1. Corrado Aaron Visaggio, Fabio Di Troia, Francesco Mercaldo, Mark Stamp, Artificial Intelligence for Cybersecurity, July 15, 2022, Springer International Publishing.
2. T. Dunning and E. Friedman, Practical Machine Learning - A New Look at Anomaly Detection, O'Reilly, 1st edition, 2014.
3. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
4. Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity, Packt Publishing, August 2, 2019, ISBN: 9781789805178, 1789805171
5. Kim-Kwang Raymond Choo, Leslie F. Sikos, Data Science in Cybersecurity and Cyberthreat Intelligence, Springer International Publishing, February 5, 2020, ISBN: 9783030387884, 3030387887

Course Outcome(CO)		Bloom's Taxonomy Level
CO1	Explain the concepts of Artificial Intelligence, Machine Learning, Deep Learning, Foundation Models, and their applications in Cyber Security	L2
CO2	Apply Machine Learning and Deep Learning techniques to	L3

	develop intelligent solutions for cyber security analytics, anomaly detection, and threat detection.	
CO3	Analyze and implement AI-driven cyber security solutions using modern AI architectures, intelligent security operations, secure AI practices, and AI risk management.	L4

CO-PO Mapping (3-High, 2-Medium, 1-Low)													
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	1	1	2	-	-	-	-	-	2	3	1
CO 2	3	2	2	2	3	1	-	-	1	-	2	3	2
CO 3	3	3	3	3	3	2	-	1	2	2	3	3	3

26CY732 CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS 2-0-3-3

Prerequisite: 26CY603 *Cryptography*

Syllabus:

Introduction to Verilog- Structure, Constructs, and Conventions. Modeling at the 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 their use. IDE and its use, FPGA-based design realizations, Design of finite field arithmetic operations, Representative designs with AES, ECC, and Hash Algorithms, Post-Quantum Cryptography (PQC) Hardware Implementations, AI-Assisted Cryptographic Hardware Design, Side-channel attacks, hardware Trojan detection, hardware security validation, PLC and SCADA security, lightweight cryptography, and security of embedded AI systems.

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. Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M., & Karri, R. (2020). *Hardware Architectures for Post-Quantum Digital Signature Schemes*. Springer International Publishing. ISBN: 978-3030576837.
6. C. K. Koc, *Cryptographic Engineering*, Springer, 2008.

Course Outcome(CO)		**Bloom's Taxonomy Level**
CO 1	Study verilog: structure, constructs, and conventions. Learn to model at the 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-	**L5**

	defined primitives, and compiler directives	
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	**L4**
CO 5	Design of finite field arithmetic operations, Representative designs with AES, ECC, Hash Algorithms, and PQC	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY741 SECURITY IN CYBER PHYSICAL SYSTEMS 3-0-0-3

Prerequisite: 26CY602 *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, Digital Twin Security, 5G/6G-Enabled CPS Security, Power grid security, critical infrastructure security, UAV and drone security, smart city security, and defense systems security.

Text Book / References

1. Danda B. Rawat, Joel J.P.C. Rodrigues, Ivan Stojmenovic, *Cyber-Physical Systems From Theory to Practice*, CRC Press 2020.
2. Fang, D., Qian, Y., & Hu, R. Q. (2023). *5G Wireless Network Security and Privacy*. John Wiley & Sons. ISBN: 978-1119784296.
3. Mourad, A., Huang, C., & others (Eds.). (2023). *Digital Twin Technologies and Smart Cities*. Springer Nature.
4. Rajeev Alur, *Principles of Cyber-Physical Systems*, MIT Press, 2015.
5. Anuradha M. Annaswamy, Pramod P. Khargonekar, Francoise Lamnabhi-Lagarrigue, Sarah K. Spurgeon, *Cyber-Physical-Human Systems: Fundamentals and Applications*, Wiley-IEEE Press 2023.

6. Liu, Yan Zhang, *Cyber Physical Systems Architectures, Protocols and Applications*, CRC Press, 2019.
7. Houbing Song, Glenn A. Fink, Sabina Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* Wiley-IEEE Press, 2017.

Course Outcome(CO)		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 with 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(3-High, 2-Medium, 1-Low)													
CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PSO 1	PSO 2	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

26CY742 STEGANOGRAPHY AND MALWARE ANALYSIS 2-0-3-3

Prerequisites: 26MA601*: 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, disassemblers, and debugger aided debugging, identifying and defeating anti-disassembly techniques, anti-debugging techniques, and code obfuscation. Windows PE file format overview, Windows API & COM overview, Malware and its mitigation strategies- viruses, worms and Trojans- Ransomwares- Polymorphic malware- Fileless malware- AI-based malware- Packers - 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. Monnappa K A. (2018). *Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware*. Birmingham, UK: Packt Publishing Ltd.

3. C. Collberg and J. Nagra, *Surreptitious Software: Obfuscation, Watermarking, and Tamper proofing for Software Protection*, Addison-Wesley, 2010.
4. Michael Sikorski and Andrew Honig, *Practical Malware Analysis*, No Starch Press 2012
5. Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sebastien Josse, *Practical Reverse Engineering*, Wiley Publishers, 2014
6. Eldad Eilam, *Reversing: Secrets of Reverse Engineering*, Wiley Publishers, 2005

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Understanding various security issues in multimedia and providing 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(3-High, 2-Medium, 1-Low)													
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	1	-	1	1	1
CO 2	1	2	2	2	2	-	-	1	1	-	1	1	1
CO 3	1	2	2	2	2	-	-	1	1	-	2	2	2
CO 4	1	2	2	2	2	-	-	1	1	-	2	2	2

24CY751 CODING AND INFORMATION THEORY 3-0-0-3

Prerequisites: 26MA601 *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 their applications, Viterbi algorithm and decoding. Machine Learning–Assisted Channel Coding, AI-Based Decoding Algorithms

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.
5. Eldar, Y. C., Goldsmith, A., Gündüz, D., & Poor, H. V. (Eds.). (2022). *Machine Learning and Wireless Communications*. Cambridge University Press.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Comprehend source coding and channel performance using Information theory	**L2**
CO 2	Apply linear block codes for error detection and correction	**L3**
CO 3	Learn cyclic codes and BCH codes for error detection and correction	**L4**
CO 4	Understand Reed-Solomon codes, convolutional codes, machine learning-based coding, and their decoding	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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 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

26CY752 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, Case study on applying formal methods for system call specification and verification.

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(CO)		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	**L2**

	verifications.	
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 with SPIN, PVS, TAMARIN, Frama-C, and Isabelle tools.	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY753 MOBILE SECURITY 2-0-3-3

Prerequisites: 26CY605*: Secure Coding*, 26CY682*: Cyber Security lab*

Syllabus

Security of Mobile Services: Mobile API Security, WebView Security, SMS Security, Location Services Security. Android App Development: Android Studio, Activities, Intents, Fragments, Data Storage, Broadcast Receivers and Content Providers, Services, Async Tasks, GPS and Maps Integration, Sensors, Connecting Web APIs, 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: Decompilation and Disassembly, Code Review, Static and Dynamic Analysis, Runtime Instrumentation, Smali Patching, Binary Patching. Native Library Exploitation. OWASP Mobile Top 10. Mobile Security Assessment: Component Analysis, Frida, HTTP Interception, SSL Unpinning and Traffic Analysis, Automated Static and Dynamic Assessment. Attacks and Vulnerabilities in Real World Android Apps (A Case Study): XSS, Task Hijacking, Code Injection, Overlay Attacks, Insecure Deep Links, Malware Analysis and ML-based Detection, App Store Security and Supply Chain Attacks, Privacy Violation, System Call Hardening, ASLR, ROP, Framework Exploits. Fuzzing for Mobile Applications. Advanced Mobile Malware and Spyware Analysis. iOS app development, Xcode, Application Security: App Store, IPA Decryption and 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.
4. *Thiel, D. (2016). iOS Application Security. No Starch Press.*

Course Outcome(CO)	**Bloom's Taxonomy Level**

CO 1	Android Application development and APK internals	**L4**
CO 2	Understanding the internals of Mobile OS and studying 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**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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	2	1	-	1	1	-	1	1	1
CO 2	2	2	2	2	2	1	-	1	1	-	2	2	2
CO 3	2	2	2	2	2	1	-	1	1	-	2	2	2
CO 4	2	2	2	2	2	1	-	1	1	-	2	2	2
CO 5	2	2	2	2	2	1	-	1	1	-	2	2	2

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

Prerequisite: *26CY681 Internet Protocol Lab*

Syllabus:

Threats to Wireless networks, Attacks on 802.11 networks – WEP, WPA, Wireless clients, Attacks on Bluetooth networks, 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 and 6G security, and IoT wireless protocols, 6LoWPAN security, Vehicle-to-Vehicle (V2V) security, Vehicle-to-Infrastructure (V2I) security, OTA update security, small-cell security, AI for wireless 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.
7. Liyanage, M., Ahmad, I., & Ylianttila, M. (Eds.). (2022). *Security in 5G and Beyond*. Wiley.

Course Outcome(CO)		**Bloom's Taxonomy Level**
CO1	Analyze Threats to Wireless Networks and Attacks on	**L4**

	802.11.	
CO2	Familiarize with Attacks and mitigation strategies for various wireless networks.	**L4**
CO3	Explore the security in Bluetooth, 5G, 6G security, and IoT wireless protocols	**L3**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY755 **Security in AI** **2-0-3-3**

Prerequisites: *26CY731 – AI for Cyber Security Applications*
Syllabus

Foundations of Generative AI and Secure AI Systems: Introduction to Generative AI, Foundation Models, Transformer Architecture, Self-Attention Mechanism, Embeddings and Vector Representations, Large Language Models (LLMs), Prompt Engineering, Fine-Tuning Techniques, Parameter-Efficient Fine-Tuning (PEFT), LoRA, Retrieval-Augmented Generation (RAG), Vector Databases, AI Agents and Autonomous Systems, Internet of Agents, Model Context Protocol (MCP), Secure AI Development Lifecycle, Model Hardening, Identity, Traceability and Secure Communication for AI Agents, Applications of Generative AI in Cyber Security. **AI Security and Trustworthy AI:** AI Threat Landscape, AI Attack Surface, Security, Privacy and Trustworthiness in AI, AI Risk Management, Threat Modelling for AI Systems, Adversarial Machine Learning, Responsible AI, AI Governance and Ethics, Robust Machine Learning, Adversarial Training, Defensive Techniques, Secure Data Pipelines, Privacy-Preserving Machine Learning, Differential Privacy, Federated Learning Security, Secure Multi-Party Computation, Homomorphic Encryption, Explainable AI, Adversarial Attacks, Privacy Attacks, Model Extraction and Inference Attacks, MITRE ATLAS Framework, AI Supply Chain Security, Model Fingerprinting, Machine Unlearning, Model Provenance and Lineage, AI Bill of Materials (AI-BoM), Security of Deep Learning Models, AI Assurance and Case Studies in AI Security. **Security of Foundation Models and Large Language Models:** Foundation Model Security, Large Language Model Security, Prompt Injection, Jailbreaking, Prompt Leakage, Hallucinations, Data Leakage, Model Theft, Security of Fine-Tuning, Security of Retrieval-Augmented Generation (RAG), Security of AI Agents and Autonomous Systems, Offensive AI for Security Evaluation, AI Hardening and Defensive Prompting, Input Validation, Output Guardrails, AI-assisted Security Operations, AI Security Frameworks and Standards, Secure AI Framework (SAIF), ISO/IEC 42001, NIST AI Risk Management Framework, EU AI Act, AI Compliance and Governance.

Text Books

1. Ian Goodfellow, Yoshua Bengio and Aaron Courville, Deep Learning, MIT Press, 2016.

2. Christopher M. Bishop and Hugh Bishop, Deep Learning: Foundations and Concepts, Springer, 2024.
3. Yevgeniy Vorobeychik and Murat Kantarcioglu, Adversarial Machine Learning, Morgan & Claypool Publishers, 2018.
4. Chip Huyen, AI Engineering: Building Applications with Foundation Models, O'Reilly Media, 2025.
5. Battista Biggio and Fabio Roli, Adversarial Machine Learning, Springer.

References

1. NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, 2023.
2. OWASP Foundation, OWASP Top 10 for Large Language Model Applications.
3. Jay Alammar and Maarten Grootendorst, Hands-On Large Language Models, O'Reilly Media, 2024.
4. Nicolas Papernot et al., Practical Black-Box Attacks Against Machine Learning, ACM AsiaCCS.
5. OpenAI, Anthropic, Google DeepMind and Meta AI Technical Reports on Foundation Model and LLM Security.
6. MITRE, MITRE ATLAS - Adversarial Threat Landscape for AI Systems.
7. ISO/IEC 42001:2023, AI Management System.
8. Google, Secure AI Framework (SAIF).

Course Outcome(CO)		Bloom's Taxonomy Level
CO1	Explain the fundamental concepts of Generative AI, foundation models, Large Language Models (LLMs), and secure AI systems.	**L3**
CO2	Analyze security, privacy, trustworthiness, and adversarial threats in AI systems using appropriate AI security principles and techniques.	**L4**
CO3	Apply AI security frameworks, defensive techniques, and governance practices to develop and evaluate secure, trustworthy AI applications	**L4**

CO-PO Mapping (3-High, 2-Medium, 1-Low)

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	3	1
CO 2	3	2	2	2	3	2	-	-	2	-	2	3	2
CO 3	3	3	3	3	3	2	-	1	2	2	3	3	3

26CY761 SECURITY IN CLOUD COMPUTING 2-0-3-3

Prerequisite: 26CY602 *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*. Cloud Security Posture Management (CSPM), Cloud Native Application Protection Platform (CNAPP), Secure Access Service Edge (SASE), Cloud Ransomware Protection, Multi-Cloud Security, Cloud HSMs, sustainable cloud security, and Post-Quantum Cryptography (PQC) adoption in cloud environments

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.
1. J. Dean and S. Ghemawat, *MapReduce: simplified data processing on large clusters*, Commun., ACM 51, no.1, 107-113, 2008.
1. 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.
2. T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly Series, 2009.
3. T. Erl, R. Puttini and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*, Prentice Hall, 2013.
4. M. Ben-Ari, *Principles of Concurrent and Distributed Programming*, Addison- Wesley/Pearson, 2nd Edition, 2006.
5. George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair, *Distributed Systems: Concepts and Design*, 5th Edition, 2011.
6. L. Rice, *Container Security: Fundamental Technology Concepts that Protect Containerized Applications*. Sebastopol, CA, USA: O'Reilly Media, 2020.

Course Outcome(CO)		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 the Hadoop cloud computing framework	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY762 SPECIAL TOPICS IN CRYPTOGRAPHY 3-0-0-3

Prerequisite: 26CY603*: Cryptography*, 26CY612*: 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, Quantum Key Distribution (QKD), Quantum 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. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th Anniversary ed.). Cambridge University Press.
7. Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*, V4, 2017.
8. *Rings and Integer Lattices in Computer Science*, lecture notes from the Bellairs-McGill workshop on Computational Complexity in 2007.

Course Outcome(CO)		**Bloom's Taxonomy Level**
CO 1	Understanding the NP hard problems on Lattices	**L2**
CO 2	Understanding the hardness of code-based cryptography	**L4**
CO 3	Understanding homomorphic encryption and its applications	**L4**
CO 4	Evaluation of Identity-based cryptosystems and functional encryption	**L4**

CO 5	Understand the concepts of Secure Multi-party computation-Visual Cryptography, Quantum Key Distribution (QKD), Quantum Cryptography	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY763 BLOCKCHAIN TECHNOLOGY 2-0-3-3

Prerequisites: *26CY603: Cryptography***,** *26CY602: Network Security*, *26CY613: Concepts in System* Security

Syllabus:

Distributed Ledger Technology (DLT), Evolution and Structure of Blockchain, Blockchain Generations, Introduction to Cryptocurrencies, Cryptographic Primitives, Hash Functions, Merkle Trees, Digital Signatures, Crypto Wallets and MetaMask Wallet, Bitcoin Architecture, UTXO Model, Mining, Consensus Mechanisms: Proof of Work (PoW), Proof-of-Knowledge systems, Altcoins, Blockchain Types: Public, Private, Consortium and Hybrid Blockchains, Ethereum Architecture, Ethereum Virtual Machine (EVM), Gas Mechanism, ERC-20 and ERC-721 Tokens, Consensus Mechanism), Proof of Stake (PoS), Introduction to Decentralized Finance (DeFi) and NFTs, Smart Contracts and Lifecycle, Solidity Programming: Structure, Data Types, Functions, Access Modifiers, Events, Mapping, Arrays, Inheritance, Error Handling, Remix IDE, Web3.js, Decentralized Applications (DApps), Introduction to Hardhat Framework, Interplanetary File System (IPFS), Hyperledger: Design Principles, Hyperledger Fabric Architecture, Peers, Channels, MSP, Chaincode Development and Deployment using Fablo and Docker, Blockchain Applications in Finance, Healthcare, Supply Chain and Cyber Security, Attacks on Blockchain Consensus and Smart Contracts, Reentrancy Attack, Integer Overflow, Front-running, Flash Loan Attacks, Blockchain Forensics, Smart Contract Auditing Tools, Formal Verification Concepts, Smart Contract Security Case Studies, Privacy-preserving Blockchain Techniques, AI and Blockchain Integration, Green Blockchain and Emerging Trends in Web3 Technologies, Byzantine attacks, Consensus security, Eclipse attacks.

Text Book / References

1. Roger Wattenhofer, CreateSpace, *The Science of the Blockchain*, Independent Publishing Platform, 2016
2. Imran Bashir, *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*, 4th Edition, Packt Publishing, 2023.
3. Andreas M. Antonopoulos, *Mastering Bitcoin - Programming the Open Blockchain*, O'Reilly Media, Inc., 2017

4. Alex Leverington, *Ethereum Programming*, Packt Publishing Limited, 2017.
5. OWASP Smart Contract Top 10, 2025.

Course Outcome(CO)		Bloom's Taxonomy Level
CO1	Understanding basic principles of Distributed Ledger Technology	**L2**
CO2	Use of cryptographic primitives in Blockchain technology	**L3**
CO3	Development of smart contracts	**L4**
CO4	Blockchain and its use cases	**L4**
CO5	Security Analysis of Blockchain Applications	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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
CO1	2	2	2	1	2	1	-	1	2	-	1	1	1
CO2	2	2	2	1	2	1	-	1	2	-	1	1	1
CO3	2	2	2	1	2	1	-	1	2	-	1	1	1
CO4	2	2	2	1	2	1	-	1	2	-	2	2	1
CO5	2	2	2	1	2	1	-	1	2	-	2	2	1

26CY764 SECURE SYSTEMS ENGINEERING 2-0-3-3

Prerequisite*:* *26CY613 Concepts in System Security*

Syllabus:

Balancing security and usability-User authentication mechanisms, Zero Trust Architecture, Identity and Access Management (IAM). Target environment hardening and secure application deployment. Threat Modeling -STRIDE, PASTA. Risk Assessment - CVSS v4.0, Attack trees. Security Testing - Common Vulnerabilities and Exploits, Application Security Testing- SAST, DAST, IAST, RASP, AI-Augmented Security: Using LLMs for code review vs. risks of AI-generated code, Fuzzing techniques-(Coverage-guided, Structure-aware). Software security economics-logging/monitoring and operational security aspects. Infrastructure Security-Infrastructure as Code (IaC- Terraform/CloudFormation/K8s manifests) Security, Container (Docker) Security, Cluster (Kubernetes) Security, eBPF for runtime protection. Software Supply Chain Security - SBOM (SPDX, CycloneDX), VEX, SCA, OSS Licensing Models, Policy-as-Code. Enhance Detection Engineering with Agile DevSecOps - SOC tech stack, EDR, SOAR, XDR, MDR, Chaos Engineering for resilience.

Text Book / References

1. Dotson, C. (2022). *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'Reilly Media.
2. S. Garfinkel and L. F. Cranor, *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly, 2008.
3. L. Rice, *Container Security: Fundamental Technology Concepts that Protect Containerized Applications*. Sebastopol, CA, USA: O'Reilly Media, 2020.
4. Bird, Jim. "DevOpsSec: *Securing software through continuous delivery*." (2016).
5. Tim Mather, Subra Kumaraswamy, Shahed: *Cloud Security and Privacy: An Enterprise*

Perspective on Risks and Compliance, O'Reilly, 2009.
6. Anderson, Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2010.
7. M. Tehranipoor, and C. Wang, *Introduction to Hardware Security and Trust*, Springer, 2011.
8. C. W. Axelrod, *Engineering Safe and Secure Software Systems*, Artech House, 2013.
9. Antonio Borghesi and Barbara Gaudenzi: *Risk Management: How to Assess, Transfer and Communicate Critical Risks*, Springer, 2013.
10. Steve Watkins: *An Introduction to Information Security and ISO27001:2013: A Pocket Guide*, 2nd Edition, IT Governance Publishing, 2013.

Course Outcome(CO)		Bloom's Taxonomy Level
CO 1	Comprehend secure design principles and threat modeling methodologies	**L4**
CO 2	Apply secure coding practices and AI-augmented vulnerability testing. Evaluate software supply chain risks using SBOMs and compliance models.	**L3**
CO 3	Analyze cloud-native infrastructure and container security architectures. Develop automated DevSecOps pipelines and operational resilience strategies.	**L4**

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

26CY765 SPECIAL TOPICS IN CYBER SECURITY 3-0-0-3

Prerequisites: 26CY602*: Network Security,* 26CY613*: Concepts in System Security*

Syllabus:

Information Technology and IPR, Intellectual Property Law, privacy law and data protection, statistical inference in databases, Private information retrieval viewed as a database access problem, Privacy in data publishing, Virtual Private Databases, access control in databases, Privacy issues in citizen digital data, eIDAS and digital trust services, 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.

Text Book / 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.
6. M. Gertz and S. Jajodia, Handbook of Database Security-Applications and Trends, Springer, 2008.

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

CO-PO Mapping(3-High, 2-Medium, 1-Low)													
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

******

25AVP501 **Mastery Over Mind (MAOM)** **1-0-2 2**

Course Outcomes

CO01: Relate to the causes of stress in one's life.

CO02: Experiment with a range of relaxation techniques

CO03: Model a meditative approach to work, study, and life.

CO04: Develop appropriate practice of MA-OM technique that is effective in one's life

CO05: Inculcate a higher level of awareness and focus.

CO06: Evaluate the impact of a meditation technique

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.

*****

23HU601 Career Competency I 0-0-3-P/F

Prerequisite:

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:

CO01: Soft Skills - To develop positive mindset, communicate professionally, manage time effectively and set personal goals and achieve them.

CO02: Soft Skills - To make formal and informal presentations with self-confidence.

CO03: Aptitude - To analyze, understand and employ the most suitable methods to solve questions on arithmetic and algebra.

CO04: Aptitude - To analyze, understand and apply suitable techniques to solve questions on logical reasoning and data analysis.

CO5: 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.

CO6: 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

CO/PO	**PO1**	**PO2**	**PO3**	**PO4**	PO5	PO6
CO01	2	1				
CO02	2	1				
CO03	2	1				
CO04	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

*****

23HU611 **Career Competency II** **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:

CO01: Soft Skills - To demonstrate good interpersonal skills, solve problems and effectively participate in group discussions.

CO02: Soft Skills - To write technical resume and perform effectively in interviews.

CO03: Aptitude - To identify, investigate and arrive at appropriate strategies to solve questions on arithmetic by managing time effectively.

CO04: Aptitude - To investigate, understand and use appropriate techniques to solve questions on logical reasoning and data analysis by managing time effectively.

CO5: 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

CO6: 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

CO/PO	**PO1**	**PO2**	**PO3**	**PO4**	PO5	PO6
CO01	2	1				
CO02	2	1				
CO03	2	1				
CO04	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

*****

26CUL500	**INTEGRATED AMRITA MEDITATION TECHNIQUE**	**L-T-P-C 0-0-2-1**
A.	**ature of Course:** Lab/Practical	**N**
B.		**C**

ourse Description:

The course introduces students to the Integrated Amrita Meditation Technique (IAM 20), a structured practice that combines yogic stretches, regulated breathing (pranayama), and guided meditation. The course integrates both theoretical understanding and experiential practice to enhance emotional balance, stress resilience, concentration, and overall holistic development.

Aligned with United Nations Sustainable Development Goal 3 (SDG 3): Good Health and Well-Being, the course promotes preventive mental health care, emotional well-being, and sustainable lifestyle practices among students. By fostering inner stability, self-awareness, and self-regulation, the programme supports academic excellence and contributes to the development of healthy individuals and communities.

The course is expected to improve student well-being, enhance academic focus and cognitive clarity, reduce stress-related indicators, and promote compassionate and emotionally supportive culture.

C. **C**

ourse Objectives:

- To promote overall health and well-being of students.
- To train students in the structured practice of IAM 20.
- To develop emotional regulation and stress management skills.
- To encourage reflective awareness and compassionate living.

D. **C**

ourse Outcomes:

After successful completion of the course, students will be able to:

CO	Course Outcomes	Knowledge Level (Bloom's Taxonomy)
CO1	Explain principles and components of IAM 20	Understand (L2)
CO2	Demonstrate and correct meditation practice independently	Apply (L3)
CO3	Analyze personal stress patterns using meditation insights	Analyse (L4)
CO4	Evaluate personal growth through daily practice	Evaluate (L5)

E. C

O-PO Mapping: [affinity: 3 – high; 2- moderate; 1- slightly]

CO's	Program Outcomes (PO's)											Program Specific Outcomes (PSF's)		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	-	-	-	-	-	1	-	2	-	-	1	-	-	-
CO2	-	-	-	-	-	2	2	1	1	-	1	-	-	-
CO3	-	-	-	-	-	1	1	2	-	-	1	-	-	-
CO4	-	-	-	-	-	1	1	1	1	-	1	-	-	-

F. **Syllabus**

Unit 1: Foundations of Meditation (CO1)

- Meaning and purpose of meditation
- Demonstration and supervised training
- Overview of structure of IAM
- Guidance for safe and effective practice
- Importance of mental health

Unit 2: Theoretical Foundations (CO2)

- Structure and components of IAM: yogic stretches, regulated breathing, and guided meditation
- Breath–mind connection
- Integration of IAM practice into daily routine and academic life
- Application of IAM for stress management, concentration, and holistic student development

Unit 3: IAM Practical Training (CO3)

- Preparatory stretches
- Pranayama components
- Guided meditation sequence
- Corrections and common challenges

Unit 4: Integration and Transformation (CO4)

- Building daily discipline
- Research evidence in higher education
- Compassion and mindful communication

G. **Evaluation Pattern:**

Assessment	**Internal (60)**	**External (40)**
Attendance	20 Marks	
Class Participation	20 Marks	
Activity	20 Marks	
Practical Demonstration		30 Marks
Viva		10 Marks

22ADM501 Glimpses of Indian Culture 2 0 1 P/F

Introduction: Love is the substratum of life and spirituality. If love is absent life becomes meaningless. In the present world if love is used as the string to connect the beads of values, life becomes precious, rare and beautiful like a fragrant blossom. Values are not to be learned alone. They have to be imbibed into the inner sprit and put into practice. This should happen at the right time when you have vitality and strength, when your hearts are open.

The present course in value education is a humble experience-based effort to lead and metamorphosis the students through the process of transformation of their inner self towards achieving the best. Amma's nectarous words of wisdom and acts of love are our guiding principles. Amma's philosophy provides an insight into the vision of our optimistic future.

1. Invocation, Satsang and Question - Answers

2. Values - What are they? Definition, Guiding Principles with examples Sharing own experiences
3. Values - Key to meaningful life. Values in different contexts
4. Personality - Mind, Soul and Consciousness - Q and A. Body-Mind-Intellect and the Inner psyche Experience sharing
5. Psychological Significance of samskara (with e.g. From Epics)
6. Indian Heritage and Contribution and Q and A; Indian Ethos and Culture
7. Self-Discipline (Evolution and Practice) – Q and A
8. Human Development and Spiritual Growth - Q and A
9. Purpose of Life plus Q and A
10. Cultivating self-development
11. Self-effort and Divine Grace - their roles – Q and A; - Vedanta and Creation – Understanding a spiritual Master
12. Dimensions of Spiritual Education; Need for change Lecture – 1; Need for PerfectionLecture - 2
13. How to help others who have achieved less - Man and Nature Q and A, Sharing ofexperiences

REFERENCES:

1. Swami Amritaswaroopananda Puri - Awaken Children (Volume VII and VIII)
2. Swami Amritaswaroopananda Puri - Amma's Heart
3. Swami Ramakrishnanda Puri - Rising Along the Razor's Edge
4. Deepak Chopra - Book 1: Quantum Healing;Book 2: Alpha and Omega of God;Book 3: Seven Spiritual Rules for Success
5. Dr. A. P. J. Abdul Kalam- 1. Ignited Minds 2. Talks (CD)
6. Swami RamakrishnandaPuri - Ultimate Success
7. Swami JnanamritanandaPuri - Upadesamritham (Trans: Malayalam)
8. Vedanta Kesari Publication - Values - Key to a meaningful life
9. Swami Ranganathananda - Eternal values for a changing society
10. David Megginson & Vivien Whitaker - Cultivating Self Development
11. Elizabeth B. Hurlock - Personality Development, Tata McGraw Hill
12. Swami Jagatatmananda - Learn to Live (Vol.1 and 2), RK Ashram, Mylapore