

Branch Name:	IMCA
Program Code:	CS301
Course Title:	Cyber Security
Course Code:	1CS3010702T
Pre-requisite Course:	Computer Networks, Operating Systems, Programming in C/C++ or Java, Discrete Mathematics, Database Management Systems. Students need basic knowledge of network protocols, OS concepts, and programming.

Course Objective:

1. Explain security fundamentals including CIA triad, threat models like STRIDE/DREAD, and risks in cloud/IoT/social media.
2. Implement classical/symmetric/asymmetric ciphers (Caesar, AES, RSA), hashing (SHA, HMAC), and PKI/digital signatures.
3. Deploy and analyze network defenses like firewalls, IDS/IPS (Snort), SSL/TLS, IPsec VPNs, and email security (PGP/SMIME).
4. Apply access controls (RBAC/ABAC), authentication (MFA), malware analysis, and policies including BCP/DRP and wireless security.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
4	-	-	4	60	40	-	-	100

Course Contents:

Unit No	Topic	Total Hours	Weight age (%)
1	Security Fundamentals • CIA Triad and Security Goals: Confidentiality, Integrity, Availability • OSI and TCP/IP Model • Threat Landscape: Malware Types, Phishing, DDoS, Social Engineering • Vulnerabilities, Exploits, and Risk Assessment Models (STRIDE, DREAD) • Cyber Laws and Ethics: IT Act 2000/2008, GDPR Basics • Cyberspace Risks: Cloud, IoT, Social Media Attack Vectors	12	25
2	Cryptography Principles • Classical Ciphers: Caesar, Vigenère, Playfair Implementations • Symmetric Algorithms: DES, 3DES, AES Modes (ECB, CBC) • Asymmetric Cryptography: RSA, Diffie-Hellman Key Exchange • Hashing and Integrity: MD5, SHA Family, HMAC • Digital Signatures, PKI, and Certificate Authorities	11	25
3	Network Security Protocols • Firewalls: Packet Filtering, Stateful Inspection, Proxy Architectures • Intrusion Detection/Prevention: IDS/IPS (Snort, Suricata), Honeypots • Transport Layer Security: SSL/TLS Handshake, HTTPS Implementation • VPN Protocols: IPsec (AH, ESP, IKE), Site-to-Site vs Remote Access • Email and Application Security: PGP, S/MIME, DNSSEC	12	25

4	System Security and Policies - Access Control: DAC, MAC, RBAC, ABAC Models - Authentication: Password Policies, Biometrics, MFA (TOTP) - Application Vulnerabilities: Buffer Overflows, SQL/XSS Injection - Malware Analysis: Viruses, Worms, Ransomware Behaviors - Security Policies, BCP/DRP, Wireless (WEP/WPA3), Cloud Threats	11	25
---	--	----	----

Text Books:

- "Cryptography and Network Security: Principles and Practice" by William Stallings, Pearson Education, 7th Edition (2017)
- "Cryptography and Network Security" by Behrouz A. Forouzan & Debdeep Mukhopadhyay, McGraw-Hill Education, 3rd Edition (2015)
- "Network Security and Cryptography" by Bernard Menezes, Cengage Learning, 1st Edition (2010)

Reference Books:

- "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, Mike Speciner, Pearson Education, 2nd Edition (2002)
- "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar, Jan Pelzl, Springer, 1st Edition (2010)
- "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard, Marcus Pinto, Wiley, 2nd Edition (2011)
- "Network Security Bible" by Eric Cole (Editor), Wiley, 2nd Edition (2009)

List of Open Source Software/learning website:

- <https://www.cybrary.it/>
- <https://owasp.org/>
- <https://cryptohack.org>
- <https://www.hackthebox.com/>
- <https://tryhackme.com/>

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Describe CIA triad, OSI/TCP-IP models, threats (malware/phishing/DDoS), risk models (STRIDE/DREAD), and legal aspects (IT Act/GDPR).	2. Understand
CLO2	Implement and compare ciphers (Caesar/Vigenère/AES/RSA), hash functions (SHA/HMAC), and PKI/digital signatures.	3. Apply 4. Analyze
CLO3	Configure firewalls, IDS/IPS (Snort), SSL/TLS handshakes, IPsec VPNs, and secure email (PGP/SMIME/DNSSEC).	3. Apply
CLO4	Design access controls (RBAC/ABAC), authentication (MFA), analyze malware/ransomware, and develop security policies/BCP/DRP.	5. Evaluate
CLO5	Analyze security threats, vulnerabilities and cyber-attack patterns in modern systems.	4. Analyze
CLO6	Design integrated security solutions for protecting organizational networks and data.	6. Create

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CLO1	H	M	M	-	-	-	-	-	-	M	H	L	M	L
CLO2	H	H	M	M	H	-	-	-	-	M	-	L	H	M
CLO3	H	M	H	M	M	-	-	-	-	M	-	-	M	M
CLO4	H	M	M	H	M	M	-	-	-	-	M	L	H	H
CLO5	M	H	M	H	M	M	-	-	-	M	-	L	M	M
CLO6	H	H	H	H	H	M	-	-	M	M	M	L	H	H

H:High, M:Medium, L:Low