गोंय विद्यापीठ
ताळगांव पठार,
गोंय - ४०३ २०६
फोन : + ९१ - ८६६९६०९०४८

Goa University
Taleigao Plateau,Goa - 403 206
Tel : +91-8669609048
Email : registrar@unigoa.ac.in
Website : www.unigoa.ac.in

(Accredited by NAAC with Grade A+)

GU/Acad –PG/BoS -NEP/2026-27/333 Date: 14.08.2026

CIRCULAR

The University has decided to implement the Curriculum and Credit Framework for the Undergraduate Programme (CCFUP) of Bachelor of Engineering in Civil Engineering under the National Education Policy (NEP), 2020 based on All India Council for Technical Education (AICTE) and National Credit Framework (NCrF) Guidelines from the Academic Year 2024-2025 onwards.

The syllabus for Semester III & IV Courses offered under the Specialization **Cyber Security** of the **Bachelor of Engineering in Computer Science and Engineering (Artificial Intelligence and Machine Learning)** Programme, as approved by the Academic Council in its meeting held on 1st July 2026 is attached.

The Dean, Faculty of Engineering and Principals of affiliated Engineering Colleges are requested to take note of the above and bring the contents of the Circular to the notice of all concerned.

ASHWIN V LAWANDE
Digitally signed by ASHWIN V LAWANDE
Date: 2026.08.14 16:57:50 +05'30'

(Ashwin V. Lawande)
Deputy Registrar – Academic

To,

1. The Dean, Faculty of Engineering, Goa University.
2. The Principals of Affiliated Engineering Colleges.

Copy to:

1. Chairperson, BoS in Computer Engineering, Goa University.
2. Controller of Examinations, Goa University.
3. Assistant Registrar Examinations (Technical and Allied), Goa University
4. Directorate of Internal Quality Assurance, Goa University for uploading the Syllabus on the University website.

Computer Science and Engineering (Artificial Intelligence and Machine Learning)

Specialization: Cyber Security

Sr. No.	Semester	Course Code	Title of the Course	L	T	P	TCr
1.	**III**	**CYS-281**	Foundations of Networks and Cryptography	3	0	0	3
		CYS-282	Networks and Cryptography Lab	0	0	1	1
2	**IV**	**CYS-283**	Principles of Cyber Security	3	0	0	3
		CYS-284	Principles of Cyber Security Lab	0	0	1	1
4	**V**	**CYS-381**	Digital Forensics and Incident Response	3	0	0	3
		CYS-382	Digital Forensics and Incident Response Lab	0	0	1	1
5	**VI**	**CYS-383**	Threat Intelligence and Cyber Defense	2	0	0	2
		CYS-384	Threat Intelligence and Cyber Defense Lab	0	0	2	2
6	**VII**	**CYS-481**	Malware Analysis and Reverse Engineering	3	0	0	3
		CYS-482	Malware Analysis and Reverse Engineering Lab	0	0	1	1
			TOTAL	**14**	**0**	**6**	**20**

Approved by: Academic Council on 1st July 2026

SEMESTER III

Name of the Programme : **B.E. in Computer Science and Engineering (Artificial Intelligence and Machine Learning)**

Course code : **CYS-281**

Title of the course : **Foundations of Networks and Cryptography**

Number of Credits : **3(3L)**

Effective from AY :**2026-27**

Pre-requisites for the Course:	Basic knowledge of Computer Science with some exposure to programming	
Course Objectives:	This course will enable students to: • To introduce the fundamentals of data communication, network architectures, protocol layers, and Internet protocols. • To explain the design and operation of data link, network, and transport layer protocols used in computer networks. • To develop an understanding of network security concepts, cryptographic techniques, and security services. • To familiarize students with classical, symmetric, and public-key cryptographic algorithms for securing communication systems.	
Contents:	Basics Knowledge of Computers	**No of Hours**
Unit-1	**Introduction to Networks:** Data Communication, Network Topologies, Network Types, Protocol layering, TCP/IP Protocol Suite, OSI reference model. Networks Devices-NIC, Switches, Routers, Gateways. **Data Link Layer:** Design issues- Framing, Error Detection (Parity, CRC), Error Correction (Hamming Code), Simplex Stop and Wait Protocol.	**11**
Unit-2	**Network Layer:** Design Issues, Routing Algorithm-Optimality Principle, Shortest Path Algorithm, IPv4 Protocol, IP address, IPv6, Internet Control Protocol- ICMP, ARP, DHCP. **Higher-level Protocols:** TCP Header, TCP Connection Establishment, TCP Connection Release, UDP- UDP Header, difference between TCP and UDP, DNS-Namespace, Resource Records, Name Resolution, HTTP/HTTPs.	**12**
Unit–3	**Introduction to Cryptography**: OSI Security Architecture, Security Attacks – Active and Passive Attacks, Security Services, Security Mechanisms, Cryptography- Keyless, Single Key, Two-Key algorithms. **Classical Encryption Techniques:** Symmetric Cipher Model-Cryptography, Cryptanalysis and Brute Force Attack, Substitution Techniques-Ceaser Cipher, Monoalphabetic Cipher, Playfair	**11**

	Cipher, Polyalphabetic Cipher, One-time Pad, Transposition Techniques.	
Unit-4	**Block Ciphers:** Difference between Stream and Block Ciphers, Feistel Cipher, DES Algorithm. **Public-Key Cryptography:** Principles, applications, requirements of Public Key Cryptography, RSA Algorithm, Diffie-Hellman Algorithm, Concept of Hash Functions and Message Authentication code.	**11**
Pedagogy:	Interactive, reflective, and inquiry based methods, with a strong emphasis on critical thinking and problem solving skills.	
References/ Readings:	**Text Books :** 1. Andrew S. Tanenbaum, Nick Feamster, & David J. Wetherall., *Computer Networks* (6th ed.). Pearson, 2022, ISBN: 978-9356063600 2. B. A. Forouzan, *Data Communications and Networking with TCP/IP Protocol Suite*, 6th ed., McGraw Hill Education, 2022. ISBN: 9789355320940, 3. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson, 2023. ISBN: 978-9357059718. Reference Books 1. William Stallings, Data and Computer Communication, 10th Edition, Pearson Education, 2017, ISBN: 978-0133506488. 2. A. Kahate, *Cryptography and Network Security*, 4th ed. McGraw Hill Education, 2019. ISBN: 978-9353168032. 3. B. A. Forouzan and D. Mukhopadhyay, *Cryptography and Network Security*, 2nd ed., Tata McGraw-Hill Education Pvt. Ltd., 2010. ISBN: 978-0070702080.	
Course Outcomes:	On completion of the course students should be able to: CO 1. Explain the fundamentals of computer networks, protocol layering, network devices, and the TCP/IP and OSI reference models. CO 2. Describe the working of TCP, UDP, DNS, and HTTP/HTTPS protocols in network communication. CO 3. Apply fundamental cryptographic concepts and classical encryption techniques to understand information security mechanisms. CO 4. Evaluate cryptographic algorithms such as DES, RSA, and Diffie-Hellman to understand secure communication and authentication mechanisms.	

Name of the Programme : **B.E. in Computer Science and Engineering (Artificial Intelligence and Machine Learning)**

Course code : **CYS-282**

Title of the course : **Networks and Cryptography Lab**

Number of Credits : **1(2P)**

Effective from AY : **2026-27**

Pre-requisites for the Course:	Basics Knowledge of Computer, Awareness regarding any programming language like C,C++ or Python	
Course Objectives:	This course will enable students to: • Understand the operation of networking devices, TCP/IP configuration, and network communication fundamentals. • Apply data communication techniques such as framing, error detection, and routing algorithms in computer networks. • Implement classical and public-key cryptographic algorithms for secure communication. • Demonstrate mechanisms for data integrity, authentication, and secure key exchange using hash functions, MACs, and cryptographic protocols.	
Contents:	List of Experiments	**No. of Hours**
	1. Case study on Study of the basic network devices. (Repeater, Hub, Switch, Bridge, router and Gateway). 2. Configure and troubleshoot TCP/IP on Microsoft Windows Operating system. 3. Implement any Data Link Layer Framing technique 4. Implement Cyclic Redundancy Check (CRC) for error detection in data transmission. 5. Implement Ceaser Cipher. 6. Implement Monoalphabetic Cipher. 7. Implement Playfair Cipher. 8. Implement transposition technique. 9. Demonstrate working of RSA Algorithm 10. Demonstrate the working of hash functions and MAC	**30**
Pedagogy:	Interactive, reflective, and inquiry-based methods, with a strong emphasis on critical thinking and problem-solving skills.	
References/ Readings:	**Text Books :** 1. Andrew S. Tanenbaum, Nick Feamster, & David J. Wetherall., *Computer Networks* (6th ed.). Pearson, 2022, ISBN: 978-9356063600 2. B. A. Forouzan, *Data Communications and Networking with TCP/IP Protocol Suite*, 6th ed., McGraw Hill Education, 2022. ISBN: 9789355320940,	

	3. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson, 2023. ISBN: 978-9357059718. Reference Books 1. William Stallings, Data and Computer Communication, 10th Edition, Pearson Education, 2017, ISBN: 978-0133506488. 2. A. Kahate, *Cryptography and Network Security*, 4th ed. McGraw Hill Education, 2019. ISBN: 978-9353168032. 3. B. A. Forouzan and D. Mukhopadhyay, *Cryptography and Network Security*, 2nd ed., Tata McGraw-Hill Education Pvt. Ltd., 2010. ISBN: 978-0070702080.
Course Outcomes:	On completion of the course students should be able to: CO 1. Configure network settings and analyse the functions of networking devices used in computer networks. CO 2. Implement and evaluate framing, error detection techniques for reliable data communication. CO 3. Develop programs for classical cryptographic techniques including Monoalphabetic, Playfair, and Transposition ciphers. CO 4. Implement public-key cryptography, hash functions, and message authentication mechanisms to achieve secure communication.

SEMESTER IV

Name of the Programme : **B.E. in Computer Science and Engineering (Artificial Intelligence and Machine Learning)**

Course code : **CYS-283**

Title of the course : **Principles of Cyber Security**

Number of Credits : **3(3L)**

Effective from AY : **2026-27**

Pre-requisites for the Course:	Basic knowledge of Computer Networks with some exposure to Cryptography	
Course Objectives:	This course will enable students to: • To introduce the concepts, classifications, and legal aspects of cybercrime from Indian and global perspectives. • To develop an understanding of cyber threats, attack methodologies, and vulnerabilities in mobile, wireless, and cloud computing environments. • To familiarize students with common cybercrime tools, techniques, and attack vectors used by cybercriminals. • To impart knowledge of phishing, identity theft, and preventive measures for securing individuals and organizations against cyber threats.	
Contents:		**No. of Hours**
Unit-1	**Introduction to Cybercrime:** Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, Cybercrime: The Legal Perspectives, Cybercrimes: An Indian Perspective, Cybercrime and the Indian ITA 2000, Introduction to Digital Personal Data Protection Act (DPDP Act, 2023). A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. **Cyber offenses:** Introduction, How Criminals Plan the Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.	**12**
Unit-2	**Cybercrime in Mobile and Wireless Devices:**Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones. **Mobile Devices:** Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.	**12**

Unit–3	**Tools and Methods Used in Cybercrime:** Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.	**11**
Unit-4	**Phishing:** Methods of Phishing, Spear Phishing, Types of Phishing Scams, Phishing Toolkits and Spy Phishing, Phishing Countermeasures. **Identity Theft (ID Theft):** Personally Identifiable Information (PII), Types of Identity Theft, Techniques of ID Theft.	**10**
Pedagogy:	Interactive, reflective, and inquiry-based methods, with a strong emphasis on critical thinking and problem-solving skills.	
References/ Readings:	**Text Books :** 1. Godbole, N., & Belapure, S. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley, 2020. ISBN: 978-81-265-2179-1 2. D. Palit, *Cybersecurity Today*. New Delhi, India: BPB Publications, 2025. ISBN: 978-936589-375-5 **Reference Books** 1. R. K. Goutam, *Cybersecurity Fundamentals*. BPB Publications, 2021. ISBN: 978-9390684731. 2. A. Kahate, *Cryptography and Network Security*, 4th ed. McGraw Hill Education, 2019. ISBN: 978-9353168032. 3. R. Meeuwisse, *Cybersecurity for Beginners*, 2nd ed. Cyber Simplicity Ltd., 2017. ISBN: 978-1911452034. 4. William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, 4th ed., Pearson Education, 2018. ISBN: 978-0134794105.	
Course Outcomes:	On completion of the course students should be able to: CO 1. Explain the concepts of cybercrime, cybercriminal behavior, cyber laws, and information security principles from national and global perspectives. CO 2. Analyse security challenges and threats associated with mobile devices, wireless networks, cloud computing, and organizational computing environments. CO 3. Identify and evaluate cybercrime tools, attack techniques, and vulnerabilities including phishing, malware, password attacks, SQL injection, buffer overflow, and denial-of-service attacks. CO 4. Assess phishing and identity theft threats and recommend appropriate countermeasures, security policies, and best practices to protect digital assets and personal information.	

Name of the Programme : **B.E in Computer Science and Engineering (Artificial Intelligence and Machine Learning)**

Course code : **CYS-284**

Title of the course : **Principles of Cyber Security Lab**

Number of Credits : **1(2P)**

Effective from AY : **2026-27**

Pre-requisites for the Course:	Basic knowledge of Computer Networks with some exposure to Cryptography	
Course Objectives:	This course will enable students to: • Develop an understanding of common cyber threats, phishing attacks, spoofing techniques, and attack vectors used in cybercrime. • Apply network monitoring and packet analysis techniques using cybersecurity tools to understand network protocols and communication behavior. • Develop basic cybersecurity applications for network information gathering, cybercrime data analysis, and visualization. • Apply security assessment techniques to identify suspicious activities and evaluate password and authentication security mechanisms.	
Contents:	**List of Experiments**	**No. of Hours**
	1. Learn to analyze email headers and website URLs to detect phishing and spoofing attempts. 2. Case study on cyber threats and attack vectors. 3. Apply Packet Capture Techniques Using Wireshark 4. Demonstrate DNS Query and Response Analysis Using Wireshark 5. Demonstrate TCP Connection Establishment Through Packet Capture 6. Compare HTTP and HTTPS Communication Using Packet Inspection Tools 7. Apply Network Traffic Monitoring Techniques to Identify Suspicious Activities 8. Develop a program that displays IP address,hostname, and domain details of websites. 9. Create programs to read cybercrime datasets andvisualize types of attacks and frequencies. 10. Apply Password Security Techniques to Evaluate Password Strength	**30**
Pedagogy:	Interactive, reflective, and inquiry-based methods, with a strong emphasis on critical thinking and problem-solving skills.	
References/	**Text Books :**	

Readings:	1. Godbole, N., & Belapure, S. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley, 2020. ISBN: 978-81-265-2179-1 2. D. Palit, *Cybersecurity Today*. New Delhi, India: BPB Publications, 2025. ISBN: 978-936589-375-5 **Reference Books** 1. R. K. Goutam, *Cybersecurity Fundamentals*. BPB Publications, 2021. ISBN: 978-9390684731. 2. A. Kahate, *Cryptography and Network Security*, 4th ed. McGraw Hill Education, 2019. ISBN: 978-9353168032**.** 3. R. Meeuwisse, *Cybersecurity for Beginners*, 2nd ed. Cyber Simplicity Ltd., 2017. ISBN: 978-1911452034. 4. William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, 4th ed., Pearson Education, 2018. ISBN: 978-0134794105.
Course Outcomes:	On completion of the course students should be able to: CO 1. **Identify** and **assess** common cyber threats, phishing attacks, and attack vectors affecting digital systems. CO 2. **Perform** network traffic capture and protocol analysis using cybersecurity monitoring tools. CO 3. **Develop** basic cybersecurity applications for network information gathering and cybercrime data analysis using programming tools. CO 4. **Apply** security assessment techniques to evaluate password strength and identify suspicious activities for improving cybersecurity practices.