WEST BENGAL COUNCIL OF HIGHER SECONDARY EDUCATION

SYLLABUS FOR CLASS XI AND XII

SUBJECT: CYBER SECURITY

Course Description:

This course introduces students to the fundamentals of cybersecurity, focusing on understanding common threats, security principles, and best practices.

Course Objectives:

The objectives of this course are to equip students with a comprehensive understanding of various aspects of cybersecurity, including:

1. Understanding of basic principles, terminology, and concepts of cybersecurity and its importance in today's digital world.
2. Understanding of common cyber threats and vulnerabilities.
3. Understanding different security technologies, tools, and techniques used to protect systems, networks, and data.
4. Exploring ethical considerations and legal regulations related to cybersecurity, including privacy laws, intellectual property rights, and ethical hacking principles.
5. Promoting awareness and education about cybersecurity best practices.

Course Outcomes:

Upon successful completion of this course, the student shall be able to:

1. Demonstrate an understanding of cybersecurity fundamentals
2. Demonstrate an understanding of the threat landscape
3. Demonstrate familiarity in cybersecurity technologies
4. Develop skills in cybersecurity
5. Demonstrate an understanding of Cryptography
6. Demonstrate familiarity of cyber security ethical issues, laws and regulations

Class – XI
Semester - I

Subject: Cyber Security

Course Code: Theory

Full Marks – 35 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1.	**Computer Systems**		**25**	**15**
	1.1	Evolution of Computers: ● Different Generations of Computers ● Brief Idea about Quantum Computers	2	1
	1.2	Computer Organization: ● Logic Gates with Truth Tables: AND, OR, NOT, X-OR ● Functional Components of a Computer System and their Interconnections ● Memory Organization (Diagrams Only) and Its Types ● I/O Devices	3	2
	1.3	Encoding Schemes and Number System: ● ASCII, EBCDIC ● Binary, Octal, Hexadecimal Number Systems	3	2
	1.4	Data and Information: ● Definitions ● Understanding the difference between data and information (through examples) ● Types of Data	2	1
	1.5	Operating Systems: ● Roles and Functions of Operating Systems ● Types of Operating Systems ● Concepts of Processes, Threads ● Memory Management (Basic Concepts) ● File Systems	3	2

	1.6	Database Management Systems: ● Overview of databases, and their importance in modern computing ● Role of DBMS in managing data ● Relational Databases ● Structured Query Language (SQL)	3	2
	1.7	Programming a Computer: ● Algorithms (Pseudocodes) ● Flowcharts ● Compiler, Interpreter ● Programming Languages (Examples) ○ C, C++ ○ Python, Java, Java-Script ● Introduction to Python Programming (Simple Example Based) ○ Python Installation ○ Basic Structure ○ Conditional Constructs ○ Looping Constructs ○ Arrays, Lists, Sets ○ Functions	9	5
2.	**Computer Networks**		**25**	**15**
	2.1	Types of Networks: ● LAN, MAN, WAN ● Wireless LAN ● Internet	2	1
	2.2	Components of a Network: ● Servers and Workstations ● Network Interface Cards ● Guided Media: Cables – UTP, STP, Co-axial, Fibre Optic ● Unguided Media: Infra-Red, Radio and Microwave Communication, Satellite, ● Repeaters, Hubs, Bridges, Switches, Routers, Gateways	4	2
	2.3	Network Topologies: Mesh, Ring, Bus, Star, Tree or Hybrid	1	1
	2.4	Concept of Channel, Bandwidth (Hz, KHz, MHz), and Data Transfer rate (bps, Kbps, Mbps, Gbps, Tbps)	1	1

	2.5	The Internet: ● History and Evolution of Internet ● TCP/IP Protocol Stack, Functionality and Protocols of each layer ● MAC Address ● IPv4 Class A, Class B, Class C Address ● Concept of Subnet Mask and Default Gateway ● IPv6 Address (Basic Format) ● ICMP	8	5
	2.6	Internet Applications: E-mail, WWW, Domain Name Systems	3	1
	2.7	Internet of Things: ● The architecture of IoT systems ● Types of IoT devices (sensors, actuators, gateways, etc.) ● Communication protocols used in IoT networks (MQTT, CoAP, Zigbee)	3	2
	2.8	Cloud Computing: ● Brief Introduction to ○ Cloud Service Models (IaaS/PaaS/SaaS) ○ Cloud Deployment Models (Public/Private/Hybrid), ● Overview of cloud storage services ● Overview of major cloud service providers (e.g., AWS, Azure, Google Cloud)	3	2
3.	**Introduction to Cybersecurity**		**10**	**5**
	3.1	Overview of Cybersecurity and Its Relevance	1	0
	3.2	History of Cybersecurity: Major Incidents and Their Impacts	2	0
	3.3	CIA Triad: Confidentiality, Integrity and Availability	1	1
	3.4	Important Terms and Definitions: Security, Privacy, Threats, Vulnerabilities, Exploits, Risks, Attacks, Attack Vectors, Hackers, Crackers	3	2

	3.5	Cyber Threats and Its Classifications: ● Malware ● Social Engineering ● DoS/DDoS ● Insider Threats ● Advanced Persistent Threats (APTs) ● Data Breaches and Information Theft	3	2

Note: Additional 10 hours for Remedial and/or Tutorial Classes

Class – XI
Semester - II

Subject: Cyber Security

Course Code: Theory

Full Marks – 35 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1.	**Network Security**		**25**	**15**
	1.1	Overview and Importance	1	0
	1.2	Network Access Control: ● Authentication Mechanisms - Passwords, Biometrics, Hardware Tokens ● Authorization and Access Control Lists (ACLs)	3	2
	1.3	Firewalls: ● Role of Firewalls in Network Security ● Types of Firewalls: Packet-Filtering Firewalls, Stateful Inspection Firewalls ● Firewall Architectures: Host-Based Firewalls Network-Based Firewalls ● Firewall Configuration and Management: Configuring Basic Firewall Rules with Linux IPTables ● Network Address Translation (NAT)	6	4

	1.4	Intrusion Detection Systems (IDS): ● Overview and Importance ● Types of IDS: Host-Based IDS, Network-Based IDS ● IDS Architectures: Centralized IDS, Distributed IDS ● Detection Techniques: Signature Based, Statistical Anomaly Detection Based (Various Features like User Login Time, Duration etc.) ● IDS Configuration and Management: IDS Sensor Configuration and Rule Creation using Snort	6	4
	1.5	Wireless Network Security: ● Overview of Wireless Security Vulnerabilities ● Securing Wi-Fi Networks - WPA2, WPA3	2	1
	1.6	IoT Security: ● Common security threats targeting IoT devices ● Attack Vectors in IoT Ecosystems: Device Compromise, Data Interception, Denial of Service (DoS), etc. ● Case Studies of Notable IoT Security Breaches ● Privacy Considerations in IoT Deployments	4	2
	1.7	Cloud Security: ● Common Security Threats to Cloud Environments ● Security in Cloud Storage	3	2
2.	**Cryptography - Part I (Without any Mathematical Derivations or Proofs)**		**25**	**15**
	2.1	Introduction: ● Overview ● Encryption and Decryption Function ● Plain Text, Cipher Text ● Symmetric Cipher Models: Substitution Ciphers, Transposition Ciphers ● Steganography	5	3

	2.2	Secret Key Cryptography: ● Symmetric Key Encryption ● Block Cipher, Traditional Block Cipher Structures ● Data Encryption Standard (DES), Example of DES, Strength of DES ● Advanced Encryption Standard (AES), Example of AES, Strength of AES ● Block Cipher Modes of Operations ● Stream Cipher ● Synchronous and Asynchronous Stream Cipher ● Autokey Stream Cipher ● RC4 Stream Cipher	14	8
	2.3	Public Key Cryptography: ● Principles of Public Key Cryptography ● RSA Algorithm with Examples	6	4
3.	**Internet Security**		**10**	**5**
	3.1	Social Engineering ● Overview and Importance ● Common Techniques: Phishing, Pretexting, Baiting, Vishing (Voice Phishing), Smishing (SMS Phishing)) - with Real Life Examples ● Impersonation ● Case Studies of Successful Social Engineering Attacks: Banking Frauds, Social Media Related Frauds/Blackmailing, Fake Profiles, Fake Videos ● Best Practices Against Social Engineering Attacks	6	3
	3.2	Email Security: ● Email Threats - Spamming, Spoofing, Phishing, Spear Phishing, Malware Distribution, Credential Harvesting - with Real Life Examples ● Email Security Best Practices	4	2

Note: Additional 10 hours for Remedial and/or Tutorial Classes

Class – XI

Subject: Cyber Security

Course Code: Practical

Full Marks – 30 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1.	**Laboratory Experiments**		**60**	**25**
	1.1	Computer Fundamentals: ● Visit to Computer Lab and familiarization with computers and peripherals and different networking devices (e.g., modem, switch, router). ● Opening of the CPU box/cabinet and identification of different parts (e.g., Motherboard, CPU/Processor, RAM, Hard Disk, power supply).	4	0
	1.2	Familiarity with Linux Operating Systems: ● Basic Commands ● Creating New Users, Setting Passwords ● Configuring Network Settings	4	0
	1.3	Python Programming Practices ● Simple programs involving conditional and loop constructs ● Socket Programming ○ TCP and UDP Sockets	20	10

	1.4	Laboratory Experiments using Wireshark: ● Capturing Network Traffic: ○ Set up Wireshark to capture network traffic on a specific interface (e.g., Ethernet, Wi-Fi). ○ Filter captured traffic based on IP addresses, protocols, or ports. ○ Analyze captured packets to identify different types of network communication (e.g., HTTP, DNS, TCP, UDP). ● TCP Handshake and Data Transfer: ○ Capture TCP traffic to observe the TCP handshake process. ○ Analyze TCP flags (SYN, ACK, FIN) and sequence numbers exchanged during the handshake. ○ Monitor TCP data transfer ● UDP Communication Analysis: ○ Capture UDP traffic to observe communication between client and server applications. ○ Analyze UDP packets to identify source and destination ports, as well as payload contents. ○ Understand the differences between TCP and UDP in terms of reliability and connection-oriented nature.	12	5

	1.5	Laboratory Experiments using IPTables: ● Basic Firewall Configuration: ○ Set up a Linux system with IPTables installed. ○ Create a basic firewall configuration to allow all outgoing traffic and block all incoming traffic. ○ Test the firewall by attempting to access services from external hosts and verify that incoming connections are blocked. ● Allowing Specific Traffic: ○ Modify the firewall configuration to allow specific types of incoming traffic (e.g., SSH, HTTP, HTTPS). ○ Use IPTables rules to open ports for allowed services while still blocking all other incoming traffic. ○ Test the firewall by connecting to allowed services from external hosts and verify that connections are permitted. ● Denying Specific Traffic: ○ Configure IPTables rules to deny specific types of incoming traffic (e.g., ICMP ping requests, Telnet). ○ Testing the firewall and verification of connections.	8	4
	1.6	Laboratory Experiments using Snort: ● Configuring Snort ○ Configure Snort to operate in either IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) mode. ○ Set up Snort to monitor a specific network interface for incoming network traffic. ● Writing and Testing Snort Rules: ○ Create custom Snort rules to detect specific network traffic patterns or signatures. ○ Test the effectiveness of the rules by generating sample network traffic that matches the defined signatures.	8	4

	1.7	Laboratory Experiments using OpenSSL: ● Encrypt a file using symmetric encryption (e.g., AES) with OpenSSL. ● Decrypt the encrypted file using the corresponding decryption key.	4	2
3.	**Viva**			**5**

Class – XII
Semester - III

Subject: Cyber Security

Course Code: Theory

Full Marks – 35 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1.	**Web Security**		**18**	**10**
	1.1	Basics of Web: ● HTTP ● Static and Dynamic Web Pages ● Layers of the Web Stack: Client-Side, Server-Side, and Database	3	2
	1.2	Web Browser Security: ● Components of Web Browser: Rendering Engine, JavaScript Engine, Networking Stack, etc. ● Common Vulnerabilities in Web Browsers: (Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Clickjacking, etc.) ● Security Features in Modern Web Browsers: Same Origin Policy (SOP), Content Security Policy (CSP), Sandboxing, etc. ● Cookies ● Browser Security Settings: Privacy Settings, Cookie Handling, Pop-up Blockers ● Addons and Plugins	12	6
	1.3	Secure HTTP ● Risks Associated with HTTP ○ Data Interception ○ Eavesdropping ○ Man-in-the-Middle Attacks ● Role of HTTPS in Protecting Sensitive Information	3	2

2.	**Malicious Software**		**17**	**10**
	2.1	Malware Types: Virus, Worms, Trojans, Spyware, Adware, Key-logger, Ransomware	5	2
	2.2	Common Methods of Malware Propagation: ● Email Attachments ● Malicious Websites ● Removable Media ● File Sharing Networks ● Malvertising ● Software Vulnerabilities ● Watering Hole Attacks ● Botnets	6	4
	2.3	Protection against Malware: ● Antivirus/Antimalware Software ● Regular Software Updates ● Email Filtering ● Web Filtering ● Least Privilege Access ● Network Segmentation ● Data Backup and Recovery ● Strong Passwords and Multi-Factor Authentication (MFA)	6	4
3.	**Mobile Device Security**		**25**	**15**
	3.1	Types of Mobile Devices: Mobile Phones, Tablets, Wearable Devices	1	0
	3.2	Privacy Concerns and Data Collection: ● Privacy Concerns Related to Mobile Device Usage ○ Location Tracking and Geolocation Data ○ Device Identifiers and Unique Identifiers (UDIDs) ○ Personalized Advertising and Data Monetization Practices ● Risks of Data Collection and Sharing by Mobile Apps and Service Providers on User Privacy.	8	4
	3.3	Mobile App Security: ● Security Implications of Mobile Apps ● Mobile App Permission Management and Best Practices ● Risks of Location-Based Social Networks	4	3

	3.4	Data Security on Mobile Devices: ● Importance of Data Security on Mobile Devices to Protect Sensitive Information. ● Risks of Unencrypted Data Storage, and Communication on Mobile Platforms. ● Benefits of Device Encryption, Secure Messaging Apps, and Encrypted Storage Solutions.	4	2
	3.5	Network Security Risks: ● Security Risks of Unsecured Wi-Fi Networks and Public Hotspots. ● Man-in-the-Middle Attacks, Wi-Fi Spoofing	3	2
	3.6	Physical Security Threats: ● Types of Physical Security Threats to Mobile Devices: Theft, Unauthorized Access. ● Strategies for Protecting Mobile Devices Physically ○ Device Passcodes and Biometric Authentication ○ Remote Tracking and Wiping Capabilities ○ Secure Device Storage and Carrying Practices	4	3
	3.7	Safe Disposal of Mobile Devices	1	1

Note: Additional 10 hours for Remedial and/or Tutorial Classes

Class – XII
Semester - IV

Subject: Cyber Security

Course Code: Theory

Full Marks – 35 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1	**Cryptography - Part II**		**25**	**15**
	1.1	Hash Functions and Its Applications: ● Definition ● Security properties of hash functions ● Example of hash functions ● Secure Hash Algorithm (SHA) ● Applications of hash functions ○ Message Authentication ○ Digital Signature ○ Other applications (one-way password files, intrusion detection, virus detection, etc.)	10	7
	1.2	Digital Signatures: ● Definition ● Properties of digital signatures ● Types of attacks against digital signatures ● Requirements for digital signature designs ● RSA signature, Example of RSA signature	5	3
	1.3	Digital Certificates: ● Public Key Certificates ● Details of X.509	4	2
	1.4	SSL/TLS: ● SSL/ TLS architecture ● SSL/ TLS handshake, Authentication ● Choice of algorithms in SSL, Choice of algorithms in TLS ● Vulnerabilities in SSL	6	3

2	**Ethical Hacking**		**15**	**10**
	2.1	● Definition of ethical hacking ● Types of ethical hacking ● Five phases of ethical hacking ● Roles and responsibilities of ethical hackers	2	1
	2.2	Information Gathering (Reconnaissance): ● Active information gathering ● Passive information gathering ● Scanning (active information gathering) ● Web reconnaissance (passive information gathering)	6	4
	2.3	System Hacking ● System hacking concepts ● Cracking passwords ● Escalating privileges ● Hiding files and covering tracks	4	3
	2.4	Spoofing ● Definition of spoofing ● Email, IP, and DNS spoofing	3	2
3.	**Ethical and Legal Considerations**		**15**	**10**
	2.1	Cyber Ethics	2	1
	2.2	Use of Trusted Software	1	1
	2.3	Intellectual Property Rights	2	1

	2.4	Cyber Law and IT Act ● Introduction to Indian Cyber Law ● Distinction between Cyber Crime and Conventional Crime ● Cyber Criminals and their Objectives ● Kinds of Cyber Crime: ○ Cyber Stalking; ○ Cyber Pornography; ○ Forgery and Fraud; ○ Crime Related to IPRs; ○ Cyber Terrorism; ○ Computer Vandalism etc. ● Penalties & Offences under the IT Act ● Offences under the Indian Penal Code, 1860 ● Cyber Crime under the Special Act ○ Online Sale of Drugs under NDPS Act ○ Online Sale of Arms under Arms Act	8	6
	2.5	Digital Personal Data Protection Act	2	1
4.	**Emerging Trends**		**5**	**0**
	4.1	Artificial Intelligence and Machine Learning in Cybersecurity	2	0
	4.2	Brief Idea of Block-Chain Technology	1	0
	4.3	Impact of Generative AI in Cyber Security	1	0
	4.4	Quantum Cryptography	1	0

Note: Additional 10 hours for Remedial and/or Tutorial Classes

Class – XII

Subject: Cyber Security

Course Code: Practical

Full Marks – 30 **Contact Hours - 60 Hours**

			Contact Hours	Marks
1.	**Laboratory Experiments**		**40**	**15**
	1.1	Laboratory Experiments using Python Scapy Library: ● Packet Crafting and Manipulation: ○ Use Scapy to craft custom packets with specific headers, payloads, and options. ○ Experiment with modifying packet fields (e.g., source/destination IP addresses, TCP flags, ICMP types) to understand their impact on network communication. ● Packet Sniffing and Analysis: ○ Use Scapy to capture network traffic on a local network interface. ○ Analyze captured packets to extract information such as source/destination IP addresses, protocols, packet sizes, and payload contents.	16	6

	1.1	Laboratory Experiments using Wireshark: ● HTTP Traffic Analysis: ○ Capture HTTP traffic between a client and server using Wireshark. ○ Analyze HTTP request and response headers to understand the communication flow. ○ Extract and view the contents of HTTP messages, including URLs, headers, and payloads. ● DNS Resolution Analysis: ○ Capture DNS traffic to observe DNS query and response messages.	12	5
	1.1	Laboratory Experiments using OpenSSL: ● Generate a digital signature for a file using OpenSSL and a private key. ● Verify the digital signature using the corresponding public key. ● Generate a self-signed certificate authority (CA) certificate and private key. ● Issue server and client certificates signed by the CA.	12	4
2.	**Project**		**20**	**10**
3.	**Viva**			**5**

Subject: Cyber Security

Class XI
Total Theory Marks: 70

Class XI Semester 1 Topics: (MCQ) Marks: 35 [1 Marks per Question]

Unit	Topic	Marks Allotted
1	Computer Systems	15x1=15
2	Computer Networks	15x1=15
3	Introduction to Cybersecurity	5x1=5
	Total	**35**

Class XI Semester 2 Topics: [Short Answer Questions, Descriptive Questions] Marks: 35

Unit	Topic	Short Answer Type Questions (2 Marks)	Descriptive Type Questions (3/4/5 Marks)	Total Marks Allotted
1	Network Security	3x2=6	1x4=4 1x5=5	15
2	Cryptography - Part I	2x2=4	1x3=3 2x4=8	15
3	Internet Security	1x2=2	1x3=3	5
	Total	**12**	**23**	**35**

Subject: Cyber Security

Class XII
Total Theory Marks: 70

Class XII Semester 3 Topics: (MCQ) Marks: 35 [1 Marks per Question]

Unit	Topic	Marks Allotted
1	Web Security	10x1=10
2	Malicious Software	10x1=10
3	Mobile Device Security	15x1=15
	Total	**35**

Class XII Semester 4 Topics: [Short Answer Questions, Descriptive Questions] Marks: 35

Unit	Topic	Short Answer Type Questions (2 Marks)	Descriptive Type Questions (3/4/5 Marks)	Total Marks Allotted
1	Cryptography - Part II	3x2=6	1x4=4 1x5=5	15
2	Ethical Hacking	2x2=4	2x3=3	10
3	Ethical and Legal Considerations	1x2=2	2x4=8	10
4	Emerging Trends	0	0	0
	Total	**12**	**23**	**35**