Course Descriptions for the Bachelor of Cybersecurity Program

Course #	Course Description
11000	**Computer Skills Placement Test** **Pre-requisites: -** The exam must cover all topics taught in the Computer Skills course (11100). Students must pass this exam to be able to enrol in the Introduction to Computer Science course (11102). If a student is unable to pass this exam, they are required to enrol in the Computer Skills – Remedial (11100) before they can register for the course (11103).
11100	**Computer Skills (Remedial)** **Pre-requisites: -** **credit hours: 0** This course aims to develop learners' ability to use computers in various aspects of their lives. The course introduces the primary concepts of computers, and the basics of using a GUI-based desktop operating system and office productivity tools including word processing, spreadsheets, and presentation applications, in addition to basics of to using emails and navigating through the world wide web. At the end of this course, the students are expected to be able to use desktop computer for everyday tasks.
11102	**Introduction to Computer Science** **Pre-requisites: -** **credit hours: 3** Introduction to computer science. Components of PC and Data representation. Low level data representations (Binary, hexa, octal, conversions, Binary Arithmetic). Introduction to programming computers. Evolution of programming languages and techniques. Problem solving by computers. Flowcharts. Problem solving through analysis and then through an introduction to programming language (Basic program structure, main function, I/O control structures, Functions, Arrays and Structures).
11103	**Structured Programming** **Pre-requisites: 11102** **credit hours: 3** This course aims to introduce the fundamentals of structured programming using a high-level programming language. Topics include concepts of structured programming, program design, development. Syntax and semantics of the presently adopted language so that students will develop the ability to program in the language. Basic elements of the language: variables, constants, and data types. Basic input/output functions. Conditional and iterative control structures. Functions (or methods) and parameter passing. Recursive functions (or methods). References and dynamic variables. Basic data structures: one and two-dimensional arrays, string manipulation and structure. At the end of this course, students are expected to be able to analyse a computing problem, design, and implement a solution using a high-level programming language.

11151	**Structured Programming Lab** **Co-requisites: 11103** **credit hours: 1** This course aims to build practical skills for structured programming using a high-level programming language. At the end of this course, students are expected to be able to analyse a computing problem, design, and implement a solution using a high-level programming language.
15110	**Cybersecurity Fundamentals** **Pre-requisites: 11102** **credit hours: 3** This course aims to provide a comprehensive knowledge of security principles and practices of information systems. Topics include an overview of security terminology (threats, attacks, security mechanisms and services including confidentiality, integrity, availability, and others), fundamentals of number theory (primes, elementary operations, modulo arithmetic), cryptography (classical, symmetric, and asymmetric cryptography), user authentication, access control, cybersecurity defense systems (IDS, IPS, Firewalls), malicious software, virtualization (concept of virtualization, virtual machines, installing and configuring Windows/Linux OSs in VM). At the end of this course, students are expected to be familiar with the concepts of protecting computing infrastructures from cyber security threats and attacks.
15200	**Programming for Security Professional** **Pre-requisites: 11103** **credit hours: 3** The course aims to introduce a recent programming language that is proper to security professional. Topics include Flow control, Strings, Lists, Tuples, Files, Functions, Modules, and Packages, input output and file handling, Object Oriented Programming features: Classes, Objects, Inheritance, Operator Overloading, Errors and Exceptions, Regular expressions, Multithreading, Modules to handle multidimensional data. Networking: Socket module, Port Scanning, Packet Sniffing, Traffic Analysis, TCP Packet Injection, Log analysis. HTTP Communications with built in Libraries, Web communications with the Requests module, Forensic Investigations: geo-locating, recovering deleted items, examining metadata and windows registry. At the end of the course, students expected to be able to deal with security problems using this resent language.
15201	**Programming for Security Professionals Lab** **Co-requisites: 15200** **credit hours: 1** This course aims to practice object-oriented programming main concepts and paradigm, with focusing on the definition and use of classes along with the fundamentals of object-oriented design. Topics include practicing classes and objects, encapsulation, constructors and destructors, composition, dynamic memory allocation, inheritance, polymorphism and operator overloading. At the end of this course, the students are expected to be familiar with main principles and concepts related to object oriented programming. Where they can write, build, debug and test their programs. In addition to use their built classes in different projects

11213	**Data Structures and Algorithms for Cybersecurity** **Pre-requisites: 15200** **credit hours: 3** This course aims to describe, explain, and implement abstract data types, including lists, stacks, queues, trees, heaps, sets, maps, hash tables, and graphs. Implement a variety of algorithms for searching and sorting, including linear search, binary search, insertion sort, selection sort, merge sort, quick sort, and heap sort. Write recursive algorithms and understand when recursion is and is not appropriate. Analyze the time and space efficiency of data structures and algorithms and apply this analysis to select the best data structure for solving particular problems. The course covers general problem-solving techniques, including divide-and-conquer, greedy, and dynamic programming. At the end of this course, the student should be able to choose the appropriate data structures and design techniques and use them to write algorithms for a specific problem.
11223	**Database Fundamentals** **Pre-requisites: 15200** **credit hours: 3** This course aims to introduce the fundamentals of database systems design and implementation. Topics include basic concepts of databases, DBMS components, data modelling, entity relationship diagrams, relational databases, database integrity constraints, relational algebra, query languages, dependencies, schema designs, normalization, and redundancy elimination. At the end of the course, students are expected to be familiar with many of the principles and concepts related to databases and how these are applied in real database systems.
11335	**Operating System** **Pre-requisites: 11213** **credit hours: 3** This course aims to introduce the fundamental of Operating System (OS) design and implementation. In this course, students will explore the importance of the operating system and its functions. Topics include an overview of the modern operating systems, types of operating systems, operating system structures, process management and threads (concepts of, communication, synchronization and deadlock), CPU scheduling, memory management and virtual memory, file systems, I/O systems and security and protection. Some topics in this course are implemented by witting programs to practically know how. At the end of this course, the students are expected to be familiar with many of the principles and concepts related to most of the actual operating systems and how these are applied in real OSs.

15220	**Networks Fundamentals** **Pre-requisites: 15110** **credit hours: 3** This course aims to understand the various aspects of data communications and computer networking systems. This is the first course on data communication networks, their architecture, principles of operations, and performance analyses. Topics include principles of data transmission and networking, network models (TCP/IP and OSI models), data signalling techniques (Analog and Digital), transmission media and the physical layer, the data link layer (principles, framing, error, and flow control, data link protocols, MAC sublayer, and channel allocation), network devices, network layer (internetworking): IP protocols/addressing, routing protocols and forwarding, and application layer (Introduction, client-server/peer-to-peer architectures, protocols including HTTP, FTP, DNS, others), and wireless networking fundamentals. By the end of the course, students will have developed a strong understanding of computer networks, their components, and their underlying technology. They will be able to design and implement basic computer networks, including setting up network devices, and monitoring network performance. They will also be able to troubleshoot network issues and perform network maintenance.
15261	**Secure Web Design and Development** **Pre-requisites: 15200** **credit hours: 3** This comprehensive course introduces students to the essentials of web design, internet programming, and web security. The course covers various aspects of web design, programming, and security, including potential threats, vulnerabilities, and best practices for mitigating security risks. Topics include: web application architecture, principles of web design, responsive design, client-side and server-side programming languages (such as HTML, CSS, JavaScript, PHP, and Python), secure coding practices, input validation and sanitization, authentication and authorization mechanisms, and session management. The course also explores web security standards and protocols (such as HTTPS, SSL/TLS, and OWASP). The course delves into common web vulnerabilities and attacks, such as SQL injection, Blind SQL Injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and clickjacking, JavaScript and Cookies Attack, Attacking Application Logic, Recent Attack Trends, Shared Hosting Vulnerabilities, Application Server Vulnerabilities. By the end of the course, students will have a solid understanding of web design, internet programming, and security principles, allowing them to design, develop, and secure visually appealing and functional web applications effectively.
15262	**Secure Web Design and Development Lab** **Co-requisites: 15261** **credit hours: 1** This lab course provides students with hands-on experience in designing, developing, and securing web applications. It covers web design principles, programming languages, secure coding practices, and web security standards. The lab exercises focus on web design principles, client-side and server-side programming languages (such as HTML, CSS, JavaScript, PHP), secure coding practices, input validation and sanitization, authentication and authorization mechanisms, and session management and learn how to identify and mitigate common web vulnerabilities and attacks, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and clickjacking.

15310	**Cryptography** **Pre-requisites: 15200 + 20234** **credit hours: 3** This course introduces the principles and practices of cryptography. Students will learn the fundamental concepts of encryption, decryption, and cryptographic protocols used to secure digital communications. Topics covered in the course include: number theory, cryptography terminology, history, and types of cryptography. Symmetric Key Cryptography: Data encryption standard (DES), advanced encryption standard (AES), and block cipher modes of operation. Asymmetric Key Cryptography: RSA, Diffie-Hellman, and ElGamal Cryptosystems. Cryptographic Hash Functions: MD5, SHA. Digital Signatures: RSA signatures, Digital Signature Algorithm (DSA), ElGamal signature schemes. Cryptanalysis: Attacks on cryptosystems, cryptanalysis techniques, and key management. The course will also include practical exercises to allow students to implement and analyze cryptographic algorithms. By the end of the course, students will have a solid understanding of the principles and practices of cryptography and will be able to design, implement, and analyze cryptographic algorithms for secure communications.
15312	**Database Security** **Pre-requisites: 11223** **Credit Hours: 3** This course will provide an overview of database security concepts and techniques. The topics will cover database security concepts, Security Architecture, Authentication: Administration of Users, Profiles, and Password Policies. Authorization: Privileges, Roles, Introduction to PL/SQL and Advanced PL/SQL (Cursors and Triggers), Virtual Private Database (VPN), Auditing, Database Encryption, Transparent Data encryption. The course also covers advanced topics such as database management security issues such as securing the DBMS, enforcing access controls, and related issues.
15313	**Database Security Lab** **Co-requisites: 15312** **Credit Hours: 1** This course introduces database design and creation using a DBMS product. Emphasis is on data modelling, and creation of simple tables, queries, view, and trigger. By the end of the course, students should be able to design and implement and evaluate secure database structures by creating simple database tables, queries.

15321	**Network and Protocol Security** **Pre-requisites: 15220 + 15310** **Credit Hours: 3** This course provides a thorough investigation into the field of network security and protocols, introducing students to the breadth of network vulnerabilities and potential threats. The curriculum incorporates various security protocols such as SSL/TLS, IPSec, PGP, VPNs and SCTP, while also exploring the significance of Access Control, Authorization, antivirus systems, and content filtering. An in-depth examination of firewall technologies, Intrusion Detection Systems, and the role of intruders and malicious software will be undertaken. The course will cover the increasingly important area of IoT and wireless sensor network security and the effective use of network scanning tools. Aspects of network performance such as Congestion Control and Quality of Service will be considered, along with Network Management principles via SNMP. By offering a historical and contemporary perspective on cyber threats, the course aims to equip students with a comprehensive understanding of network security measures, preparing them to design, implement, and manage secure networks in various IT contexts.
15322	**Network and Protocol Security Lab** **Co-requisites: 15321** **Credit Hours: 1** This extensive lab aims to study and practice common computer and network security techniques and protocols. Topics include hands-on on network devices (Switches, Routers, Access Points, Firewalls, IDSs/IPSs, Repeaters/Hubs, NICs), building a small LAN using proper cabling and connection, the use of packet tracer to develop, configure and simulate a small/medium size network topology making use of different active networking components, configuring VLANs, NATs, DHCP, and VPNs, applying different Internet and routing protocols, using and configuring firewalls/IDS, Installing and configuring Server OS to implement several security policies, Installing and using Microsoft Azure to create and monitor Cloud applications. In addition to using some other tools to test, monitor, and document wired and wireless networks. The students will also set up scenarios in the real testbed, collect and analyze the results, and write lab reports about the experiments.
15350	**Artificial Intelligence and Data Analytics** **Pre-requisites: 20134 + 20233** **Credit Hours: 3** This course aims to familiarize students with computational intelligence techniques and adopt them in the system (i.e., network) hardening/defense and anomaly detection (implementing IDS/IPS). Topics include an introduction to artificial intelligence (AI), neural networks, fuzzy logic systems, machine learning algorithms, threat identification, behaviour, assessment and analysis, data/attack analytics, analysing network traffic Wireshark tool, security threats intelligence, performance measures (system metrics), and threat hunting. This course introduces the concept of evading and poisoning intelligent detection systems that provide improved network traffic monitoring/analysis, help minimize exposure (attack surface and vectors), and improve system availability.

15361	**Secure Systems Development and Design** **Pre-requisites: 11223** **Credit Hours: 3** In this course, Students will learn the importance of integrating security into all phases of the software development lifecycle, including requirements gathering, design, implementation, testing, and deployment. Topics include: threat modelling, secure coding techniques, secure design principles, input validation, output encoding, authentication and authorization, session management, error handling, logging and monitoring, and security testing. Emphasis is on practices and patterns that reduce or eliminate security breaches in software intensive systems, and on testing systems to expose security weaknesses. By the end of the course, students will have the knowledge and skills needed to design and develop secure software systems, effectively reducing the risks associated with common vulnerabilities and design flaws. The course incorporates industry best practices, including the Open Web Application Security Project (OWASP) Top Ten and the IEEE "Avoiding the Top 10 Software Security Design Flaws".
15381	**Infrastructure Security using Linux (ISL)** **Pre-requisites: 11335** **Credit Hours: 3** This course provides an overview of infrastructure security using Linux. The course will cover the following topics: principal security operations of Linux, Linux Security Modules (LSM), hardening Linux kernel and system, and Infrastructure security for securing components using Linux, such as Linux VPN (site-site and remote access), firewalls, routers, and switches. Server security, including the best practices for securing Linux servers (patching, access control, and intrusion detection). Monitoring and auditing (Linux AAA), including the tools and techniques for monitoring and auditing Linux systems (log management and vulnerability scanning). Security services include web, file, mail, data center, CA, DNS, and mobile device/application management (MDM/MAM). Throughout the course, students will engage in hands-on lab exercises to apply the concepts and techniques learned in the course. By the end of the course, students will have gained practical experience in securing Linux infrastructure components. They can design, implement, and evaluate Linux security solutions for various applications.
15382	**Auditing Policies, Legal, Ethics, Compliance** **Pre-requisites: 15312** **Credit Hours: 3** This course provides an overview of the policy, legal, ethics, and compliance issues that are relevant to cybersecurity professionals. The course will cover the following topics: Best practices of work ethics in the field of cybersecurity for organizations and individuals, issues related to the ethics and practices of using social media platforms, national and international legislation to combat cybercrimes, judicial authorities, agreements, treaties and international organizations related to cybersecurity, compliance frameworks and standards: National and international cybersecurity standards and controls (e.g. Cybersecurity Framework for Jordan Banking Sector and Cybersecurity Controls issued by the National Cyber Security Center, HIPAA, ISO 27001, PCI DSS, SOX), international cybersecurity law and policy, incident response and reporting requirements, privacy and data protection legislation and regulations (e.g. GDPR), intellectual property protection legislation and regulations, guidelines and best practices in recent trends (e.g. BYOD, Internet of Things protection guidelines), best practices for aligning with cybersecurity legislation, controls and standards.

15410	**Data Integrity and Authentication** **Pre-requisites: 15310** **Credit Hours: 3** This course aims to provide an in-depth exploration of data integrity and authentication, including the principles and best practices for ensuring data accuracy, completeness, and authenticity. The course will cover the following topics: Overview of data integrity and authentication. data integrity techniques including data redundancy, checksums, and error-correcting codes, message authentication codes (HMAC, CBC-MAC), digital signatures, authenticated encryption and hash trees. Authentication techniques including techniques for authenticating data and users, authentication strength (passwords authentication, cryptographic tokens, biometrics authentication, multifactor authentication, and One-Time passwords and knowledge-based authentication). Password attack techniques: dictionary attack, brute force, rainbow table, phishing, and social engineering attacks. Password storage techniques: cryptographic hash functions, collision resistance, salting, iteration count and password-based key derivation. Advanced protocols such as Zero-knowledge proofs. Verification analysis (Formal and Informal). By the end of the course, students will have gained practical experience in ensuring data integrity and authenticity and will be able to design, implement, and evaluate data protection solutions for various applications.
15411	**Digital Forensics and Incident Response (DFI)** **Pre-requisites: 11335** **Credit Hours: 3** This course serves as general introduction to the field of digital forensics. It covers several fundamental topics in the area of digital forensics investigations, including file, disk, network, wireless, database, malware, email, memory and mobile forensic. In addition, the course introduces students to the best practices and standards related to the incident response. By the end of the course, students will have gained a deep understanding of digital forensics and incident response and will be able to design, implement, and evaluate effective response strategies for various incidents and evaluate effective response strategies for various incidents.
15412	**Digital Forensics and Incident Response Lab** **Co-requisites: 15411** **Credit Hours: 1** In this lab, the students will practice digital forensics using the most commonly tools used in the field. The students will learn and practice the basics of forensics, deal with evidence media and environment, collect evidence, apply validation techniques, evaluate forensic methodologies, conduct evidence analysis, report and present outcomes of forensic investigation. By the end of this lab, students will have gained practical experience in designing and implementing digital forensics and incident response solutions for various applications.

15433	**Malware Analysis and Reverse Engineering** **Pre-requisites: 11335** **Credit Hours: 3** This course will introduce students to modern techniques in malware analysis through readings and hands-on interactive analysis of real-world samples. Topics include an overview of the computer system, X86 microprocessor architecture, assembly language (16-bit), addressing modes & machine codes, malware analysis primer, malware analysis in virtual machines, static malware analysis, dynamic malware analysis, reverse engineering (overview, X86 disassembly, the IDA Pro, recognizing C code constructs in assembly, analysing malicious windows programs, X86 Debugging), malware behaviour, malware encoding (obfuscation and encryption). At the end of this course, the students will be equipped with the skills to analyse contemporary malware using static and dynamic analysis. Students will learn how to analyse malicious software using reverse engineering concepts safely and thoroughly. This analysis aims to understand malicious software's behaviour and potential security impacts.
15453	**Ethical Hacking and Penetration Testing (EHT/PENT)** **Pre-requisites: 15411** **Credit Hours: 3** This course covers common methods used in ethical hacking and penetration testing to detect and protect systems from attacks. The course covers both theoretical and practical aspects of ethical hacking and penetration testing, and emphasizes the design and implementation of effective testing strategies. Topics include foot-printing, reconnaissance, system scanning, cracking passwords, network hacking (DoS Attack, Sniffing, Spoofing, Session Hijacking), web-hacking (SQL Injection attacks, Cross-Site Scripting attacks, Cross-Site Request Forgery attack etc.), social engineering, and escalating privileges. In all cases, students will learn how to write reports and apply remedial techniques. By the end of the course, students will have gained a deep understanding of ethical hacking and penetration testing and will be able to design, implement, and evaluate effective testing strategies for various applications.
15483	**Information Systems Risk Management** **Pre-requisites: 15382** **Credit Hours: 3** This course introduces information systems risk management, including risk identification, risk assessment and analysis, insider threats, risk measurement and evaluation models and methodologies, and risk control. The course will cover the following topics: risk management lifecycle and steps, cyber risk assessment and analysis methodologies, methodologies for measuring and evaluating cyber risks, cyber risk management standards and frameworks, cyber risk management processes across levels in the organization, cyber risks mitigation economics, transference, acceptance and mitigation of cyber risks, cyber risks policies for technologies, risk procedures, and standards, individuals and entities, characteristics of organizations that influence cyber risk, analysis and management, communication of cyber risks, and overview of business continuity and disaster recovery, including business impact analysis, disaster recovery planning, and testing. By the end of the course, students will have gained a strong understanding of information systems risk management and be able to apply risk management methodologies and frameworks to manage risks to information systems in their organizations

15490	**Practical Training** **Pre-requisites: Finish 90 C.H** **Credit Hours: 3** The student is required to do practical training in a well-known software company for a period of (2) months, full-time training, with at least (6) hours per day, or 3 months part-time training with at least (4) hours per day. In addition to training hours, for the part-time training, the student is allowed to register not more than (10) credit hours in the first or the second semester, or (4) credit hours in the summer semester. The student is required to perform tasks that are related to his major, such as writing, developing, or learning some new software.
15491	**Graduation Project 1** **Pre-requisites: Finish 90 C.H** **Credit Hours: 1** Project is aimed at developing real-world problem-solving skills, including problem definition, analysis, and needed software. A project should be performed by a group of students under the supervision of a faculty member. Students are required to develop a complete implementation fulfilling the project objectives and submit a final report. Project must be presented to a committee of the faculty
15492	**Graduation Project 2** **Pre-requisites: 15491** **Credit Hours: 2** Project 2 aims at implementing the planned requirements, which were collected in Project 1 Students must work in groups to achieve a functional system at the end of this course. Students must test the product / system and that should be included in the documentation.
15340	**Identity Management** **Pre-requisites: 15310** **Credit Hours: 3** This course provides students with a comprehensive understanding of identity management concepts, technologies, and best practices in the context of cybersecurity. Topics Include: Identification and Authentication: People and Devices, Network Access Control (NAC), Identity Access Management (IAM), Roles, Multi-Method Identification and Authentication Systems, Biometric Authentication Systems, Accuracy/FAR/FRR, Resistance, Privacy, Usability and Tolerability of the Methods. Physical and Logical Assets Control: System Hardware, Network Assets, Backup/Storage Devices, Rules-Based Access Control (RAC), Role based Access Control (RBAC), Inventory Tracking Methods, Identity Creation Methods. Identity as a Service (IaaS), Third-Party Identity Services, Access Control Attacks and Mitigation Measures: Password, Dictionary, Brute Force, Spoofing Attacks, Multi-Factor Authentication, Strong Password Policy, Secure Password Files and Restrict Access to Systems. By the end of the course, students will have gained a solid understanding of identity management principles and practices, allowing them to design, implement, and manage effective identity management solutions for various applications.

15371	**Cyber Crimes (CCR)** **Pre-requisites: 15310** **Credit Hours: 3** This focused course on Cyber Crime aims to provide students with a comprehensive understanding of the various cybercrimes and abuses prevalent in the digital world. By exploring their impact on individuals, organizations, and society. The course will cover the following topics: Cyber Crime Types: (Intrusions, Ransomware, Espionage, Intellectual Property Theft, Fraud, Extortion, Services Disruption, Data Leakage, Data Destruction, Data Falsification), Cyber Stalking and Predators, Cyber Bullying, Identity Theft, Cyber Assisted Crimes, Cyber Terrorism, and Cyber Crime Laws: National Laws, International Laws, Treaties. After completing this course, students will be adept at identifying cybercrimes, understanding their societal impact, evaluating relevant laws, and devising strategies to tackle them.
15383	**Block chain Technology** **Pre-requisites: 15310** **Credit Hours: 3** This course provides an in-depth exploration of blockchain technology and its various applications. The course covers the fundamentals of distributed ledger technology, consensus mechanisms, authentication techniques, and relevant protocols. The course provides students with an understanding of blockchain systems such as Bitcoin and Ethereum and an introduction to alternative blockchain platforms. Through this course, students will examine real-world applications of blockchain technology, including cryptocurrencies, supply chain management, and B2B/B2C/C2C scenarios. Additionally, students will gain hands-on experience in building and deploying smart contracts and distributed applications.
15413	**Advanced Forensics** **Pre-requisites: 15411** **Credit Hours: 3** This course introduces the methodology and procedures associated with digital forensic analysis of incidents that involve internet, computer, network and mobile forensic. Topics including: configuring a secure OS using command line and graphical utilities. OS file systems architectures, security vulnerabilities, user security, hardening, data and file recovery. network data acquisition, network forensics analysis, network logs and traffic acquisition and analysis, managing Intrusion Detection/ Prevention Systems (IDS/IPS), Managing Security Incident and Event Management (SIEM) systems, etc. mobile technology, mobile devices and cellular networks then to the processes, methods and techniques of mobile forensics. Students will learn about the importance of network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. They will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur on any computer. Students will perform actual mobile forensics investigations using state-of-the-art tools: commercial and open-source.

15420	**Mobile and Wireless Security** **Pre-requisites: 15220** **Credit Hours: 3** This course focuses on the security challenges and requirements in mobile communication, wireless networks, and cellular networks. Topics include: Fundamentals to wireless and mobile security, Wireless network security protocol (e.g., WEP, WPA, WPA2, WPA3). Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications. Bluetooth, NFC, and RFID security. Cellular network security, including GSM, CDMA, 3G, 4G, and 5G security mechanisms, as well as challenges and vulnerabilities associated with these technologies. By the end of the course, students will have developed the necessary knowledge and skills to effectively secure mobile devices and wireless networks in various environments.
15422	**Multimedia Security** **Pre-requisites: 11213** **Credit Hours: 3** Multimedia Security is a comprehensive course that covers various techniques and algorithms used to secure multimedia content from unauthorized access, use, modification, or distribution. Students will learn about cryptographic techniques, watermarking, steganography, digital rights management (DRM), and emerging threats like Deep Fake. The course also includes multimedia forensics, which involves using digital forensic techniques to analyze multimedia data and identify its authenticity, integrity, and origin. Through the course, students will develop a comprehensive understanding of the principles and practices of multimedia security and learn the skills needed to develop secure multimedia applications while also exploring new technologies and tools for multimedia protection.
15423	**Cloud Computing Security** **Pre-requisites: 15321** **Credit Hours: 3** This course provides students with a comprehensive understanding of the security challenges associated with cloud computing environments. Topics include: virtualization platforms, cloud computing models (IaaS, PaaS, SaaS, DaaS), cloud service providers and their security offerings, cloud deployment models (public, private, hybrid, community), Hypervisors and Cloud Computing Implementations, risk assessment and management in cloud environments, data encryption and key management, secure access control mechanisms, securing virtualized environments, cloud security standards and certifications, auditing and monitoring in the cloud, incident response and disaster recovery planning, and legal, privacy, and regulatory compliance issues in the cloud. By the end of the course, students will have gained a solid understanding of cloud computing security concepts and best practices.

15425	**Network Programming** **Pre-requisites: 11335** **Credit Hours: 3** This course introduces students to the fundamental concepts and techniques of network programming. Topics include: network protocols and architectures, sockets programming, data communication, and network application development. TCP/IP and UDP protocols, socket programming in different programming languages (e.g., C, Java, and Python), data encoding and serialization, and network application design patterns. Students will also explore real-world examples of networked applications, such as chat servers, file transfer programs, and web services. By the end of the course, students will be equipped to design, develop, and implement secure and robust networked applications effectively.
15434	**Internet of Things Security** **Pre-requisites: 15321** **Credit Hours: 3** The Internet of Things (IoT) is a rapidly evolving field transforming how we interact with technology. The course covers the underlying technologies that power IoT networks, including sensors, embedded systems, cloud computing, and wireless communication protocols used in IoT networks (including Wi-Fi, Bluetooth, Zigbee, and cellular networks). The course will also provide an in-depth understanding of the security risks associated with IoT devices and how to mitigate them. In this course, you will learn about the different layers of IoT security, including physical, network, application, and data security, and the various security challenges associated with IoT networks, such as device authentication, data privacy, and data integrity. Students will also learn about the common threats that target IoT devices, such as malware, botnets, and distributed denial-of-service (DDoS) attacks. By the end of this course, students will have a solid understanding of IoT technology, security challenges associated with IoT networks, and the skills to secure IoT devices and networks against cyber threats.
15435	**Hardware Security** **Pre-requisites: 15310** **Credit Hours: 3** Hardware security is an important aspect of cybersecurity that deals with protecting the physical components of computing systems from unauthorized access, tampering, and exploitation. This course covers the fundamental concepts, techniques, and hardware security challenges. The course will focus on the following topics: Introduction to hardware security and its importance, Threat models and attack vectors for hardware systems, Hardware security mechanisms and countermeasures, such as encryption, access control, and physical protections, Trusted computing and secure boot processes, Side-channel attacks and defenses, Reverse engineering and tampering techniques, Hardware security testing and evaluation methodologies, and case studies of real-world hardware security breaches and their impact. By the end of this course, students will gain a comprehensive understanding of hardware security concepts and techniques and develop the skills to design, evaluate, and defend hardware systems against security threats.

15443	**Social Engineering and Human Factors** **Pre-requisites: 15110** **Credit Hours: 3** This course explores the role of human factors and social engineering in cybersecurity, emphasizing the psychological, social, and behavioral aspects that contribute to successful cyberattacks. Topics include: human factors in cybersecurity. Types of social engineering Attacks (phishing and spear phishing attacks, physical/impersonation, vishing (phone phishing), email compromise, and baiting). Psychology of social engineering attacks (adversarial thinking, how emotional responses impact decision-making, cognitive biases of risks and rewards, and trust building). Misleading users (spoofing message senders, misleading URLs, how users judge and trust webpages and emails, as well as user behaviors with phishing and other browser warnings). Detection and mitigation of social engineering attacks. By the end of the course, students will be able to identify, analyze, and mitigate social engineering threats effectively, enhancing the overall security posture of organizations.
15455	**E- Business Security** **Pre-requisites: 15261** **Credit Hours: 3** E-Business Security is a course that focuses on protecting and securing e-commerce from unauthorized access, hacking, data theft, and online fraud. This course covers a range of technologies and algorithms used to secure user data, electronic payments, and privacy protection. Students will learn about cybersecurity, encryption, software security, virus and malware protection, and how to detect and respond to breaches. The curriculum also includes a study of online fraud cases and the preventative measures taken against them. Students will also explore methods of securing networks and applications, and protecting sensitive data and intellectual property in an e-commerce environment. By the end of the course, students will have a comprehensive understanding of e-business security principles and practices and the skills to apply them in creating a secure and trustworthy e-commerce environment.
15485	**Cyber Resilience and Business Continuity** **Pre-requisites: 15382** **Credit Hours: 3** In this course, students will learn the principles and best practices for ensuring cyber resilience and business continuity in the face of various cyber threats and incidents. Topics include: understanding the relationship between cybersecurity and business continuity, incident response planning (Anticipate, Detect and Mitigate), disaster recovery planning, crisis communication, and managing the human element in cyber incidents, business continuity (Contingency Planning, Incident Response, Emergency Response, Backup and Recovery). the implementation of effective backup strategies, and the importance of testing and refining these plans regularly. By the end of the course, students will have the knowledge and skills to develop, implement, and maintain comprehensive cyber resilience and business continuity strategies, effectively reducing downtime and mitigating the impact of cyber incidents on an organization's operations.

15493	**Special Topics in Cybersecurity (1)** **Pre-requisites: Department Approval** **Credit Hours: 3** This course aims to introduce new topics in cybersecurity. A series of advanced topics in areas of cybersecurity is offered. The course details a structured discussion of varied subjects to include technological updates related to a specific track, a more intense study of topics covered in other course offerings, and an introduction to advanced concepts. The department determine the content of the course.
15494	**Special Topics in Cybersecurity (2)** **Pre-requisites: Department Approval** **Credit Hours: 3** This course aims to introduce new topics in cybersecurity. A series of advanced topics in areas of cybersecurity is offered. The course details a structured discussion of varied subjects to include technological updates related to a specific track, a more intense study of topics covered in other course offerings, and an introduction to advanced concepts. The department determine the content of the course.