



Faculty of Computer Science and Informatics

Information Technology Department

Study Plan for Bachelor's Degree in Cybersecurity 2023/2024

Study Plan Credit hours (132)

Type of Program: **Blended**

Major Type:

Humanities

Scientific/Technical

Science Medical

Teaching Type	Percentage of study plan hours/number	Actual Ratio
Complete Online E-Learning	20% - 10% Maximum	20%
Blended learning (for humanities)	60% - 40% Maximum	
Blended learning (for scientific majors)	50% - 30% Maximum	43%
Face-to-face learning (for humanities)	20% Minimum	
Face-to-face learning (for scientific majors)	30% Minimum	37%

Note: The learning types of the courses are disseminated at all academic levels in the program



Department Vision

Excellence in teaching, learning, scientific research, and community service in information fields locally and regionally.

Department Mission

Preparing qualified student competencies in the field of information technology and cybersecurity to meet the needs of the local community, through qualified cadres capable of keeping pace with local and international standards in accordance with the standards for integrating e-learning.

Department Objectives

1. Possess the necessary theoretical and applied skills and knowledge in the field of cybersecurity.
 2. Provides professional competencies and practicing their profession with confidence and the ability to compete locally and regionally.
 3. Continue learning and professional development amidst technical changes.
- Work effectively within work teams while assuming ethical and professional responsibilities and knowing the needs of society.

Learning Outcomes

Graduates of the program will have the ability to:

1. Analyze computing issues, apply principles of computer science and related fields, and find appropriate solutions

(Knowledge): Defining principles of computing and other related disciplines to identify solutions.

(Skill): Analyze computing problems to identify solutions.

2. (Skill): Design, implement, and evaluate a computing-based solution to meet a specific set of computing requirements within the context of the program specialty.

3. (Skill): Communicate effectively in a variety of professional contexts.

4. Discern professional responsibilities and make appropriate judgments about computing-based practices in accordance with ethical and legal principles.

(Knowledge): Recognition of professional responsibilities, ethical theories, legal and social issues.



(Skill): Employing cybersecurity computing practices based on legal and ethical principles.

5. Work and participate effectively as a member or team leader in activities related to the specialty.

(Competency): Work effectively as a team member or team leader participating in activities appropriate to the program specialty.

6. Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]

(Knowledge): Illustrate security principles and practices to maintain operations in the presence of risks and threats.

(Skill): Assessing the severity of security risks, threats or digital crimes to ensure continuity of operations.

(Competency): Building security knowledge and skills to maintain operations in the presence of risks and threats.

Contents of the Study Plan

The bachelor's degree program in Computer Information Systems consists of 132 credit hours distributed as follows:

No	Requirement Type	Credited Hours	Percentage
First	University Requirements	27	20%
Second	College Requirements	18	14%
Third	Program Requirements	87	66%
Total		132	100%

University Coding System

4	0	5	-	Year	Term	-	-
College Code	Department Code		Knowledge Area	Course Level		Course Sequence	
4 Faculty of Computer Science and Informatics	05 Cybersecurity						



Knowledge Areas

No	Knowledge Area	Credit Hours in the Study Plan
01	Computer Science and Algorithms: Discrete Mathematics, Data Structures, Algorithms, Operating Systems.	12
02	Programming: Advanced Programming, Web Application Programming.	6
03	Fundamentals of Cybersecurity: Fundamentals of Cybersecurity, Computer Networks, Data and Programming Security (Application), Network Security, Infrastructure Security Using Linux.	15
04	Cybersecurity: Data Analytics, Fundamentals of Artificial Intelligence, Cryptography, Digital Forensics, Data Integrity and authentication, Secure communication protocols.	15
05	Supporting Knowledge Areas: Statistics, Numerical Analysis, Linear Algebra.	6
06	Elective Courses: Several courses within the sub-field of the program.	9
–	Field training: 3 hours after passing a minimum of 80 credit hours.	3
–	Graduation Project (1): 1 credit hour after passing 90 credit hours. Graduation Project (2): 2 credit hours after passing graduation project (1)	3



First: University Requirements: (72) Credit Hours

A. Compulsory Requirements: (18) Credit Hours

Teaching type			Course Number	Teaching type	Credit Hours	Prerequisite
Online E-Learning	Blended	Face-to-Face				
✓			5051104	Communication and Communication Skills 1 (Arabic)	3	5051108
✓			5051105	Communication and Communication Skills 1 (English)	3	5051108
✓			5051108	Arabic Language Basics	0	
✓			5051109	English Language Basics	0	
✓			5051110	Computer Basics	0	
✓			5051205	Life Skills and Social Responsibility	3	
✓			5051206	National Education	3	
✓			5051305	Leadership and Innovation	3	
✓			5051308	Military Sciences	3	
			Total		18	

B. University Elective: choose (9) Credit Hours from the following courses

Teaching type			Course Number	Teaching type	Credit Hours	Prerequisite
Online E-Learning	Blended	Face-to-Face				
✓			5052106	Communication and Communication Skills 2 (Arabic)	3	5051104
✓			5052107	Communication and Communication Skills 2 (English)	3	5051105
✓			5052103	Principles of Psychology	3	
✓			5052104	Human Rights	3	
✓			5053101	Islamic Culture	3	
✓			5053105	Quds and the Hashemite Guardianship	3	
✓			5054103	Computer Skills	3	5051110
✓			5054104	Development and Environment	3	
✓			5054106	Health and Society	3	
✓			50541308	Foreign Language	3	
✓			50541309	Digital Culture	3	5051110
			Total		9	

**Second: College Compulsory Requirements: (18) Credit Hours**

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
		√	40512102	Data Structures	3	3	0	40321203
		√	40512103	Laboratory of Data Structure	1	0	3	40512102 (co)
	√		40322101	Websites Design	3	3	0	40511101
		√	40342202	Databases	3	3	0	40512102
		√	40342203	Laboratory of Databases	1	0	3	40342202 (co)
	√		50212104	Linear Algebra	3	3	0	50551105
		√	40321101	Introduction to Programming	3	3	0	
		√	40321102	Laboratory of Introduction to Programming	1	0	3	40321101 (co)
Total					18	15	3	

Third: Program Requirements (87) Credit Hours**A. Compulsory Requirements: (75) Credit Hours**

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		40571203	Communication and Writing Skills	2	2	0	
		√	40311201	Discrete Mathematics	3	3	0	50551105
	√		40511101	Fundamentals of information technology	3	3	0	
		√	40321203	Object Oriented Programming	3	3	0	40321101
		√	40321204	Laboratory of Object-Oriented Programming	1	0	3	40321203 (co)
		√	40612204	Algorithms Design and Analysis	3	3	0	40512102
	√		40543101	Data and software security	3	3	0	40322202



	✓	40322202	Programming of Internet Applications	3	3	0	403222101-40342202 (co)
	✓	40542101	Computer Networks	3	3	0	4051101
	✓	40513103	Operating Systems	3	3	0	40512102
	✓	40541201	Introduction to Cybersecurity	3	3	0	
	✓	40542102	Fundamentals of Encryption	3	3	0	40541201
	✓	40543201	System and Infrastructure Security	3	3	0	40543204
	✓	40543103	Information Security Protocols	3	3	0	40542102
	✓	40543204	Network Management and Security	3	3	0	40542101
	✓	40543205	Networks Monitoring and Certification	3	3	0	40543204
	✓	40543206	Electronic Commerce Security	3	3	0	40543101
	✓	40544108	Ethical Hacking	3	3	0	40543204
	✓	40544109	Intrusion Detection and Prevention	3	3	0	40543204
	✓	40544110	Networks and Information Security Programming	3	3	0	40543101
	✓	40544213	Digital Forensics	3	3	0	40543204
	✓	40542103	Data integrity and authentication	3	3	0	40321203
	✓	40543202	Secure Systems Development and Design	3	3	0	40543101
	✓	40543102	Cybersecurity Ethics, Risks and Policies	3	3	0	40541201
	✓	40584202	Field Training	3	3	0	Complete 80 CH
	✓	40594202	Applied Graduation Project (1)	1	1	0	Complete 90 CH
	✓	40594203	Applied Graduation Project (2)	2	2	0	40594202
			Total	75	74	1	

B. **Elective Requirements:** (9) Credit Hours

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		40544112	Wireless Network Security	3	3	0	40542101
	√		40544214	Internet of Things Security	3	3	0	40542101
	√		40544215	Cloud Computing Security	3	3	0	40543103
	√		40544216	Special Topics in Cybersecurity	3	3	0	Complete 60 CH
	√		40544217	Advanced Digital Forensics	3	3	0	40544213
	√		40544218	Penetration Testing	3	3	0	40543101
			Total		9	9	0	

C. **Fourth: Support Courses:** (3) Credit Hours

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		50551105	Principles of Mathematics and Statistics	3	3	0	
			Total		3	3	0	



Guidance plan

First Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
4051101	Fundamentals of Information Technology	Blended	3		
4032101	Introduction to Programming	Face-to-Face	3		
4032102	Laboratory of Introduction to Programming	Face-to-Face	1	4032101	
4054201	Introduction to Cybersecurity	Blended	3		
5055105	Principles of Mathematics and Statistics	Blended	3		
	University Compulsory Requirement	Online E-Learning	3		
Total			16		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
40322101	Websites Design	Blended	3	4051101	
40321203	Object Oriented Programming	Face-to-Face	3	4032101	
40321204	Laboratory of Object-Oriented Programming	Face-to-Face	1		40321203
40571203	Communication and Writing Skills	Blended	2		
40311201	Discrete Mathematics	Face-to-Face	3	5055105	
50212104	Linear algebra	Blended	3	5055105	
	University Elective Requirement	Online E-Learning	3		
Total			18		

* Credit Hours



Second Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40542101	Computer Networks	Face-to-Face	3	40511101	
40212102	Data Structures	Face-to-Face	3	40321203	
40512103	Laboratory of Data Structures	Face-to-Face	1		40512102
40542103	Data integrity and authentication	Face-to-Face	3	40321203	
40542102	Fundamentals of Encryption	Face-to-Face	3	40542101	
	University Compulsory Requirement	Blended	3		
Total			16		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40543204	Network Management and Security	Face-to-Face	3	40542101	
40322202	Programming of Internet Applications	Face-to-Face	3	40322101	40342202
40342202	Databases	Face-to-Face	3	40512102	
40342203	Laboratory of Databases	Face-to-Face	1		40342203
40543103	Information Security Protocols	Face-to-Face	3	40542102	
	University Compulsory Requirement	Online E-Learning	3		
Total			16		



Third Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40543205	Networks Monitoring and Certification	Blended	3	40543204	
40543101	Data and software security	Blended	3	40322202	
40513103	Operating Systems	Blended	3	40512102	
40612204	Algorithms Design and Analysis	Face-to-Face	3	40512102	
40543102	Cybersecurity Ethics, Risks and Policies	Blended	3	40541201	
	University Compulsory Requirement	Online E-Learning	3		
Total			18		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40544213	Digital Forensics	Blended	3	40543204	
40543201	System and Infrastructure Security	Face-to-Face	3	40543204	
40544110	Networks and Information Security Programming	Face-to-Face	3	40543101	
40543206	Electronic Commerce Security	Blended	3	40543101	
	University Compulsory Requirement	Online E-Learning	3		
	Program Elective Requirement	Online E-Learning	3		
Total			18		



Fourth Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40544109	Intrusion Detection and Prevention	Face-to-Face	3	40543204	
40543202	Secure Systems Development and Design	Blended	3	40543101	
40594202	Applied Graduation Project (1)	Blended	1	Complete 90 CH	
	University Elective Requirement	Online E-Learning	3		
	University Compulsory Requirement	Online E-Learning	3		
	Program Elective Requirement	Blended	3		
Total			16		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
40544108	Ethical Hacking	Blended	3	40543204	
40594203	Applied Graduation Project (2)	Blended	2	40594202	
40584202	Field Training	Blended	3	Complete 80 CH	
	University Elective Requirement	Online E-Learning	3		
	Program Elective Requirement	Blended	3		
Total			14		

Courses Tree



Courses Tree

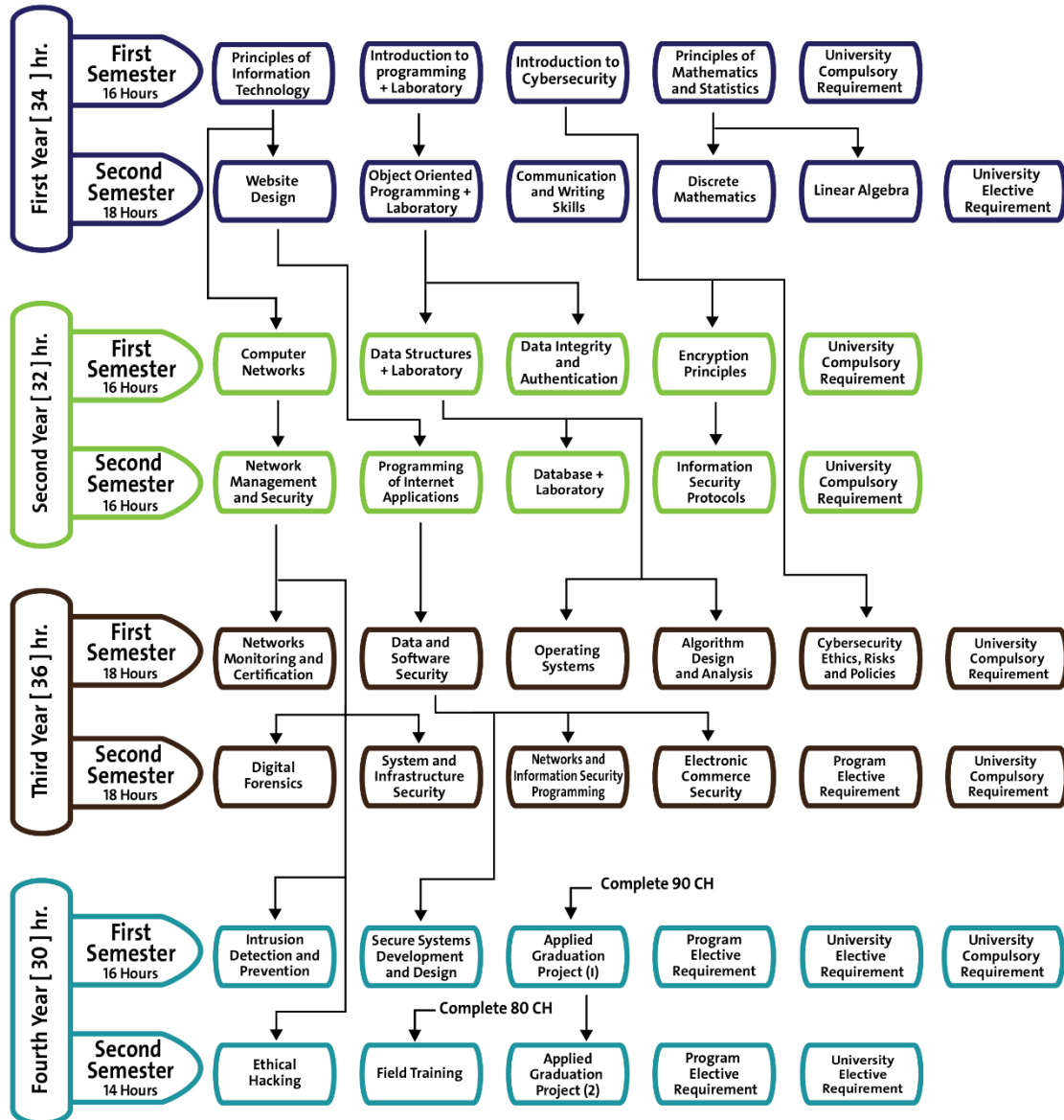
Faculty: Computer Science and Information

Department: Information Technology

Major: Cyber security Program

Program: Bachelor

Issue Date: 2023/2024



F566-1, Rev. a
Ref.: Quality Assurance Council Session (08/2021-2022), Decision No.: 01, Date: 21/05/2022



F026, Rev. c
Ref.: Deans' Council Session (24/2023-2024), Decision No.: 12, Date: 05/02/2024





Courses Description

40512102, Data Structures, (3) Credit Hours, Prerequisite: 40321203 Object Oriented Programming, Face-to-Face

Basic concepts of data structure and algorithm. The topics that will be covered in this course concerning Data type and structures; Abstract data types and encapsulation; Stacks; Queues; Recursion; Linked Lists; Binary trees; General trees; File organization: sequential and indexed files; Graphs: representation, traversing, shortest path; Sorting: exchange, insertion, quick sort, heap and others; Searching. At the end of this course, students will be able to select the proper data structure and algorithm to solve a specific software problem, the course includes complete a practical project or research by the students.

40512103, Laboratory of Data Structures, (1) Credit Hours, Co-requisite: 40512102, Face-to-Face

A practical laboratory in data structures, covering practical exercises including abstract data types and aggregation, accumulators, tuples, recursion, sequential lists, general trees, file organization, graphs, sorting and searching. The laboratory includes the completion of a practical project or research by students.

40511101, Fundamentals of Information Technology, (3) Credit Hours, Prerequisite: -, Blended

Knowledge of the terminology, information systems environment, processes, and components associated with information technology, information systems concepts, components, tools, and applications. It will provide an introductory understanding of computer hardware, numbering system and knowledge of how data is prepared for computer, instruction processed at a basic machine level, and software (operating systems, database, and web development and applications). It also introduces the networking, Internet, and the basics of the information security, web searching, in addition to algorithms and problem solving, the course includes complete a practical project or research by the students.

40342202, Databases, (3) Credit Hours, Prerequisite:40512102 Data Structures, Face-to-Face

Basic concepts of databases and the main topics such as: database definition, database system; overview of database management, database system architecture, introduction to relational model, database algebra, database design, database integrity, an introduction to structured query language (SQL), mapping between ER- and EER-to-Relational, the course includes complete a practical project or research by the students.

40342203, Laboratory of Database, (1) Credit Hours, Corequisite: 40342202, Face-to-Face

A practical laboratory in databases, covering practical exercises in database system and database management (relational database systems RDBMS, structured query language (SQL), and schema design techniques), the course includes complete a practical project or research by the students.

40311201, Discrete Mathematics, (3) Credit Hours, Prerequisite: 50551105 Principle of Statistics and Probability, Face-to-Face

Fundamental aspects of discrete mathematics used in computer science starting with propositions, logical operations, truth tables, set theory, relations and functions, and methods of proofs. The course also introduces the concepts of sequences, matrices, lattices, graph theory, and trees (rooted tree, subtree), the course includes complete a practical project or research by the students.



**40322101, Websites Design, (3) Credit Hours, Prerequisite: 4051101 Fundamentals of Information Technology, Blended**

Basic concepts of the World Wide Web, internet technology, current Web protocols, and client-server programming for desktop computers and smart phones. Students will learn standard Hypertext Markup Language (HTML) for create the web pages, basics of Cascading Style Sheets (CSS) for design and layout the web pages, as well as JavaScript, together with XML and JSON for data-interchange and Ajax technology for building rich internet applications for desktop computers and smart phones. Students will apply their gained knowledge in a series of practical assignments. At the end of this course, students will create and maintain a small web page project on a live web server for desktop computers and mobile devices.

40321101, Introduction to Programming, (3) Credit Hours, Prerequisite: -, Face-to-Face

The fundamental concepts of programming using selected language. It covers basic structures of programming concepts such as variables, data types, control structures, arrays, functions, and pointers. A brief introduction to classes and objects is also given. Students will apply their gained knowledge in a series of assignments. Practical work for three hours weekly is included. The course includes complete a practical project or research by the students.

40321102, Laboratory of Introduction to Programming, (1) Credit Hours, Corequisite: 40321101, Face-to-Face

A practical laboratory in programming using selected language, where it covers practical exercises in the basics of programming such as variables, data types, control statements, matrices, functions and indicators. In this course, students apply their knowledge through a series of practical assignments in the laboratory.

40571203, Communication and Writing Skills, (2) Credit Hours, Prerequisite: -, Blended

Concepts of administrative communication and to develop some of the skills he needs in his private life and career, in addition to his definition of the basic concepts of communication as a core and vital in the life of business organizations. To achieve this, the course will deal with the following topics: the nature, importance and objectives of the communication process, trends, elements and channels of communication, obstacles to effective communication, the basis of successful correspondence writing. In addition to the recognition of listening skills and teamwork and the management of meetings and interviews, the course includes complete a practical project or research by the students.

40321203, Object Oriented Programming, (3) Credit Hours, Prerequisite: 40321101 Introduction to Programming, Face-to-Face

Object-oriented concepts (encapsulation, data abstraction, inheritance, and polymorphism) along with OO design using UML (unified modeling language). The OOP concepts covered using JAVA programming language. The course emphasizes on the concepts of classes, templates, friend classes, inheritance, abstract class and virtual functions, exceptions, and generic programming. Upon completion, students should be able to use an object-oriented language to develop rather complex programs, the course includes complete a practical project or research by the students.

**40321204, Laboratory of Object Oriented Programming, (1) Credit Hours, Corequisite: 40321203, Face-to-Face**

A practical laboratory in object-oriented programming, covering practical exercises in object-oriented programming (encapsulation, data abstraction, inheritance, polymorphism). The course is concerned with applying concepts of classes (classes and templates, friendly classes, inheritance, abstract layer and virtual functions, exceptions and general programming in a practical way). Students will apply their knowledge through a series of practical assignments in the laboratory.

40612204, Algorithms Design and Analysis, (3) Credit Hours, Prerequisite: 40512102 Data Structures, Face-to-Face

Basic concepts of designing and analyzing algorithms. Topics covered: review of abstract data types and data structures, definition of algorithms, classifying functions and computational complexities of algorithms, algorithms analysis & design techniques including: divide and conquer greedy methods, searching and sorting, trees, graphs, hashing, combinatorial algorithms and P/NP problems, the course includes complete a practical project or research by the students.

40543101, Data and software security, (3) Credit Hours, Prerequisite: 40322202 Programming of Internet Applications, Blended

Information systems security and contemporary issues in information security and confidentiality problems, confidentiality models, methods to reduce risks and losses, information systems security within organizations, cryptography, information security control, information security programs, safe and reliable systems, user identification, network security case study. Firewall design and methods of prevention from malwares, the course includes the implementation of an applied project or research by students.

40542103, Data integrity and authentication, (3) Credit Hours, Prerequisite: 40321203 Object Oriented Programming, Face-to-Face

The course provides a comprehensive overview of the integrity and authentication of data, while emphasizing the importance of cryptography in securing data and supporting its authentication processes. The course also addresses other issues, such as hardware problems, software engineering, and the social and political challenges that must be taken into account to achieve a comprehensive and effective security system. The course includes special topics such as encryption techniques. Classic and modern, data hiding methods, and the impact of human factors on authentication systems.

40322202 Programming of Internet Applications, (3) Credit Hours, Prerequisite: 40322101 Websites Design + 40241202 Databases, Face-to-Face

The knowledge and the tools to design and implement internet web applications for desktop computers and smartphones using PHP language as a server-side language. Initially, the course will introduce HTML language and web applications. Students will learn about concepts of PHP, the functionality of web servers, and install and configure Apache HTTP server or Microsoft IIS. This course goes over the syntax and usage of PHP language such as data types, operators, arrays, control statements, expressions, sessions, cookies, as well as creating programs that interact with MySQL databases. At the end of this course, students will create and maintain a small web application project on a live web server for desktop computers and smartphones. The course includes completing a practical project or research by the students.



**40542101 Computer Networks, (3) Credit Hours, Lecture: 3, 40511101 Fundamentals of Information Technology, Face-to-Face**

Key Concepts of Computer Networks; Broad Range of Topics in Networking (e.g. Networks Applications, Network Classifications and Topologies, Network Layers, Channel Performance Measures, Transmission Media, Communication Network Protocols and Architecture); Data Link Layer (e.g. Framing, Error Detection and Correction, CSMA/CD, LAN IEEE Standards); Network Layer (e.g. IP service model, IP Addressing, Sub-netting, Host Configuration DHCP, ARP Protocol, ICMP protocol); Transport Layer (e.g. UDP Protocol, TCP Protocol, TCP Reliable Transfer and Sliding Window, TCP Flow and Congestion Control); Application Layer (e.g. DNS Protocol, NAT Protocol, HTTP Protocol, Persistent and Non-Persistent HTTP Connection), the course includes complete a practical project or research by the students.

40513103 Operating Systems, (3) Credit Hours, Prerequisite: 40512102 Data Structures, Blended

This course covers the definition and role of the operating systems. Topics spanned functionality and structuring methods of a typical operating system; Introduction to modern operating systems, including device control, interrupts, synchronization and inter-process communication, process scheduling, memory management and virtual memory, disk management, and security. Students will apply their gained knowledge in a series of assignments.

40541201 Introduction to Cybersecurity, (3) Credit Hours, Prerequisite: -, Blended

Information security evolution into cybersecurity, theory of cybersecurity, and the relationship of cybersecurity to countries, companies, society and people. Students will learn about cybersecurity techniques, processes, and procedures in which they learn how to analyze the threats, vulnerabilities, and risks present in these environments, and develop appropriate strategies to mitigate potential Cybersecurity problems.

40542102 Fundamentals of Encryption, (3) Credit Hours, Prerequisite: 40541201 Introduction to Cybersecurity, Face-to-Face

Information systems security and contemporary issues in information security and confidentiality problems, confidentiality models, in addition to dealing with methods to reduce risks and losses, information systems security within institutions, cryptography, coding basics, symmetric and asymmetric public key, hash functions, message authentication, RSA, Diffie -Hellman, CAs, digital signatures, generating false random numbers, basic protocols and their computational complexity requirements to elliptic curve coding. The course includes the implementation of an application or research project by students.

40543201 System and Infrastructure Security, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face

Physical and logical security over data centers, buildings, and offices. It also defines a management program that protects assets across all levels of technology and the core components that support that technology. In addition, it targets to analyze hacking methodology and how to create a functioning IT Infrastructure program for businesses, whether large or small, and includes change management scenarios and how to approach daily business security issues from a cybersecurity perspective.

**40543103 Information Security Protocols, (3) Credit Hours, Prerequisite: 40542102 Fundamentals of Encryption, Face-to-Face**

Contemporary security protocols and their features, including confidentiality, authentication, group security, privacy, and anonymity. It covers encryption primitive, as well as measuring models and formal tools used for mechanical validation of secure systems, including model checking, resolving constraints, algebra operation, protocol logic, and game theory.

40543204 Network Management and Security, (3) Credit Hours, Prerequisite: 40542101 Computer Network, Face-to-Face

Acquire the ability to demonstrate a deep understanding of the role of a security professional in safeguarding an organization's data against theft, damage, and disruption. In addition, the course develops the necessary skills to design, implement, and support robust security measures for network devices, ensuring the integrity of the network infrastructure. It also prepares students for a successful career in network security, equipping them with the expertise and capabilities required to meet the demands of the ever-evolving field. By achieving these course objectives, students will be well-prepared to contribute to the protection of valuable data and network assets, making them professionals in the field of network security.

40543205 Networks Monitoring and Certification, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Blended.

Concept of packet capture and its work mechanism, in addition to the concepts of packet/traffic analysis and protocol coordination. This course covers dealing with network devices specialized in network monitoring tasks, followed by conducting network monitoring in all sizes of networks, small or medium or enterprise.

40543206 Electronic Commerce Security, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Blended

E-commerce principles, business and technology topics overview, business models, and virtual value chains. Some of the major issues related to e-commerce security, privacy, intellectual property rights, authentication, encryption, fair use policies and legal obligations, client-side vulnerabilities (browsers) associated with web browsing, system penetration, information infringement and identity threats. SSL data flow encryption, data confidentiality and integrity using third-party transaction protocols such as SET, PCI DSS Standard, server-side security: CGI Security, Server Configuration, Access Control, Operating System Security, Malicious E-mail Messages, Web Scripts, Cookies, Web Bug Spyware, Web Server Architecture, Web Application Piracy, Infrastructure Mapping and Profiling, Web Authentication and Licensing, Hacking Scripts and Defensive Coding, Securing and Accessing Databases, Denying Buffer Overflow Attacks, Client Security, and Threats Modeling.

40544108 Ethical Hacking, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Blended

Principles and techniques for using hacking skills for defensive purposes, planning, investigating, surveying, exploiting, post-exploiting, reporting on results, and the possibility of exploiting system weaknesses and how to overcome these problems.

**40544109 Intrusion Detection and Prevention, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face**

Methods of intrusion detection, statistical approaches, and machine learning to detect computer attacks, network monitoring and analysis, and estimate the number and severity of attacks represented by investigations and denial of service attacks. Host-based attacks are buffer overruns. Malicious code represented by viruses and worms, in addition to identifying statistical patterns for detecting and classifying attacks. Network data visualization.

40544110 Networks and Information Security Programming, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Face-to-Face

Information and network security programming using Python introduces students to the concepts of programming using Python in addition to analyzing and designing secure networks and server systems, developing secure software using cryptography, Crypto API, hacking web applications, penetration testing, and secure network systems with a firewall and its identifiers that constitute the main tasks of a security engineer. Cyber, IT Security Programmer, and Cyber Security Analyst.

40544213 Digital Forensics, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Blended

This course will provide students with the necessary skills to become familiar with the concept of digital forensics and how to detect traces of hackers and collect the necessary digital forensic evidence in a technically and forensically sound manner to be presented in courts of law. Students will learn the basic elements, concepts, tools, techniques, and common activities of digital forensics, so that they are well prepared to participate in digital forensic investigations. You will learn how to collect digital forensic evidence from computers or mobile devices and from fixed and volatile storage media and analyze it using a series of specialized programs, with each task explaining how to use a specific tool or technology. The sources of information collection will be explained, including the importance of open source intelligence (OSINT). At the end of this course, students will present a small project using some digital forensics tools to detect and analyze forensic evidence and recover lost data.

40543202 Secure Systems Development and Design, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Blended

This course covers the principles and practices of secure and high assurance software development process, including security development lifecycle models, and design/verification/validation using languages and tools such as UML. Tools and techniques for code analysis and testing, and evaluation and certification of software will also be emphasized. It covers secure programming principles using different languages, with particular focus in secure software development. It defines and identifies vulnerability detection and avoidance. Topics include threat modeling, and the interaction between security and usability authentication, principle of least privilege, buffer overflows, race conditions, time-of-check vs. time-of-use, trust management, access control, and other relevant security issues.

40543102 Cybersecurity Ethics, Risks and Policies (3) Credit Hours, Prerequisite: 40541201 Introduction to Cybersecurity, Blended

This course focuses on the legal, ethical, and social issues associated with the use of computers and software. Professional and ethical responsibilities, civil and personal rights, the impact of computing on institutions, the ethics of using the Internet, professional ethics, means of establishing them, obstacles to their application, intellectual property rights and their protection, software piracy, institutions for monitoring software piracy and patenting of inventions. Types of information systems crimes, computer viruses, hackers and crackers, hacking, and spy files.





some economic issues in computing, monopoly and its many forms. Introduction to risk management, risk management life cycle, risk assessment and analysis techniques. Risk exposure factors, security controls and services, risk assessment and mitigation strategies, reports and consulting, and finally threat and vulnerability management.

40584202 Field Training, (3) Credit Hours, Prerequisite: Complete 80 CH, Blended

Training is required for each student in one of the organizations for not less than 8 weeks and 200 hours of training, the practice regulations are according to the training regulations issued and approved by the department, college, and dean's council of the university.

40594202 Applied Graduation Project (1), (1) Credit Hour, Prerequisite: Complete 90 Credit Hours, Blended

Phase I (Analysis and Design), the Applied project includes theoretical and practical practices related to the current problems and applications in Cybersecurity, applied research-oriented, technical report, and presentation.

40594203 Applied Graduation Project (2), (2) Credit Hours, Prerequisite: 40594202 Applied Graduation Project (1), Blended

Phase 2 (Implementation), the Applied project includes theoretical and practical practices related to the current problems and applications in Cybersecurity, applied research-oriented, technical report, and presentation.

40544112 Wireless Network Security, (3) Credit Hours, Prerequisite: 40542101 Computer Networks, Blended

Advanced topics on security and privacy of wireless communications systems, including cellular and wireless networks such as wireless body area networks, personal networks, and local area networks. This course discusses current security threats in wireless and mobile networks. The course covers modern technologies used to protect network security and discusses the design and operation of security protocols for wireless networks.

40544214 IoT Security, (3) Credit Hours, Prerequisite: 40542101 Computer Networks, Blended

The basic concepts of the Internet of Things and its future directions. The evolution of the Internet of Things, its technology and its commercial drivers and future. Giving an overview of the transition from machine-to-machine (M2M) solutions to IoT, as well as market incentives and industrial structures, IoT architecture and general design principles for different architectures, technological basics for building and implementing M2M and IoT solutions. A view of IoT security, IoT ethics and privacy. In addition to building automation and security, relevant case studies of vulnerabilities and security attacks on the Internet of Things, mitigation controls, and IoT applications represented by asset management, industrial automation, commercial building automation, smart cities, and participatory sensing, the course includes the completion of an application or research project by students.

40544215 Cloud Computing Security, (3) Credit Hours, Prerequisite: 40543103 Information Security Protocols, Blended

Concepts of cloud computing and architectural principles, design techniques and patterns and best practices in the real world applied to cloud service providers and consumers and providing secure cloud-based services, as well as cloud security architecture and exploration of guiding security design principles, design patterns, industry standards, and application technologies and addressing regulatory compliance requirements of critical importance to design, implement and manage cloud-based services.



**40544216 Special Topics on Cybersecurity, (3) Credit Hours, Prerequisite: Complete 60 CH, Blended**

Special topics on current trends in Cybersecurity, the course includes completing a practical project or research by the students.

40544217 Advanced Digital Forensics, (3) Credit Hours, Prerequisite: 40544213 Digital Forensics, Blended

The methodology and procedures associated with digital forensic analysis of incidents that involve the internet, computer, network, and mobile forensics. Topics include configuring a secure OS using the 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, 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.

40544218 Penetration Testing, (3) Credit Hours, Prerequisite: 40543101 Data and Software Security, Blended.

Learn how hackers compromise operating systems and evade antivirus software. This course will teach the student how to discover the weaknesses in the network by using the same mindset and methods as hackers. The students will acquire the skills to test and exploit your defenses and implement countermeasures to reduce risk in your enterprise. This course will cover the stages of penetration testing including reconnaissance, scanning, gaining access, maintaining access, and covering tracks and types of attacks.

50551105 Principles of Mathematics and Statistics, (3) Credit Hours, Prerequisite: -, Blended

Introduction to functions, limits and continuity, derivatives and rules, and techniques of differentiation. It introduces also the science of statistics and statistical research methods, sampling, and sample data collection and classification. It covers various topics in descriptive statistics, correlation and regression analysis, time series, and index numbers, the course includes completing a practical project or research by the students.

50212104 Linear Algebra, (3) Credit Hours, Prerequisite: 50551105 Principles of Mathematics and Statistics, Blended

Introduction to numerical analysis, and its primary objective is to develop the basic understanding of numerical algorithms and the required skills to implement algorithms to solve mathematical problems, the course includes completing a practical project or research by the students.