

**JORDAN UNIVERSITY OF SCIENCE  
AND TECHNOLOGY**

**Faculty of computer and information technology  
(CIT)**

**Cybersecurity Department**

**Study Plan of bachelor's degree in  
Cybersecurity**

## **Important Contacts**

### **Jordan University of Science and Technology**

P.O. Box: 3030 Irbid 22110 Jordan

Tel: (962)-2-7201000

Fax: (962)-2-7095141

E-mail: [prsdj@just.edu.jo](mailto:prsdj@just.edu.jo)

### **Department of Cyber Security**

Tel: (962)-2-7201000 Ext: 23903

Fax: (962)-2-7095046

E-mail: [aiiad@just.edu.jo](mailto:aiiad@just.edu.jo)

### **Admission and registration unit**

Tel: (962)-2-7201000 Ext: 27134

Fax: (962)-2-7201027

E-mail: [register@just.edu.jo](mailto:register@just.edu.jo)

### **Faculty of Computer and Information Technology**

Tel: (962)-2-7201000 Ext. 20000

Fax: (962)-2-7095046

E-mail: [cit@just.edu.jo](mailto:cit@just.edu.jo)

### **Deanship of Students affairs**

Tel: (962)-2-7201000 Ext: 23508

Fax: (962)-2-7201043

E-mail:

[studentaffairs@just.edu.jo](mailto:studentaffairs@just.edu.jo)

### **International Students Office**

Tel: (962)-2-7201000 Ext: 23040

Fax: (962)-2-7201025

E-mail: [iso@just.edu.jo](mailto:iso@just.edu.jo)

## **Vision**

To fill the Cybersecurity gap by adopting novel approaches in our one-of-a-kind undergraduate Cybersecurity program.

## **Mission**

Our mission is to provide students with introductory-level cybersecurity know-how, and along the way, it progresses to advanced cybersecurity technologies intended to help various industries and organizations to secure their networks, protect their data regimes, and find solutions against hackers, and mitigate everyday cyber vulnerabilities against cybercrimes.

## **Program Objectives**

- Develop, deliver, and implement inter-disciplinary undergraduate curricula in the domain of cybersecurity to support the next generation of cybersecurity professionals for academia and practice.
- Develop the infrastructure necessary to support research and education in the areas of security analytics, ethical hacking, network security, and secure programming.
- Build competencies on cybersecurity to advance the field of ethical hacking and penetration testing by developing new methods for discovering vulnerabilities and issues in computer systems and networks.
- Initiate government and industry partnerships for research, education, and training.

## **Graduates of the program will have the ability to:**

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]

## **Course Numbering Convention:**

<b>Digit</b>	<b>Meaning</b>	<b>Explanation</b>	
Hundreds	Course Level	1	First year
		2	Second year
		3	Third year
		4	Forth year
Tens	Course Subject	0	Basic Principles
		1	Programming
		2	Database
		3	-
		4	Networks
		5	Applications
		6	Information Hiding
		7	Systems and Systems Software
		8	Miscellaneous
9	Special Topics and Training		
Ones	Course Sequence	Course sequence number within subject area	

## Study Plan for the Cybersecurity Program 2021

A Bachelor of Science (B.Sc.) degree in Cybersecurity at Faculty of Computer and Information technology at JUST is awarded in accordance with the statute stated by JUST regulations for B.Sc. awarding issued by the Dean's Council based on 1987 law for awarding scientific degrees and certifications at JUST after completing (132) credit hours successfully, distributed as indicated in the following table:

**Table (1)**

Requirements	Mandatory	Elective	Total
University Requirements	16	9	25
Faculty Requirements	24	0	27
Departmental Requirements	71	12	80
Total	111	21	132

### **1. University Requirements (25 CHs) classified as:**

- 1-a) University Mandatory Courses (16 CHs).
- 1-b) University Elective Courses (9 CHs).

### **2. Faculty Requirements (24 CHs) shown in table (2):**

**Table (2): Mandatory Faculty Requirements**

Course Number	Course Title	Credit Hours	Weekly Hours		Prerequisite	Teaching Mode
			Lecture	Lab		
MATH 101	Calculus I	3	3	0	-	Face To Face
MATH 102	Calculus 2	3	3	0	Passing MATH 101	Face To Face
MATH 241	Discrete Mathematics	3	3	0	-	Face To Face
CS 101	Introduction to Programming	3	2	0	CIS 99 or Concurrent	Face To Face
SE 103	Introduction to Information Technology	3	3	0	Concurrent with CS 101	Online (Synchronous)
SE 112	Introduction to Object-Oriented Programming	3	2	0	Passing CS 101	Hybrid (1+1)
CS 211	Data Structures	3	3	0	MATH 241+ passing SE 112	Hybrid (1+1)
CIS 221	Fundamentals of Database Systems	3	3	0	CS 211	Face To Face

### 3. Department Requirements (80 CH) classified as:

#### 3-a) Department mandatory requirements (71 CH):

**Table (3): Mandatory Department**

Course Number	Course Title	Credit Hours	Weekly Hours		Prerequisite	Teaching Mode
			Lecture	Lab		
CY 101	Cybersecurity Fundamentals	3	3	0	CS 101	Face To Face
CY 111	Assembly Language Laboratory	1	0	3	CS 112 (or concurrent)	Face To Face
CY 201	Cybersecurity Ethics	1	1	0	CY 101	Online (Synchronous)
CY 211	Selected Visual Programming Language	2	0	6	CS 112	Hybrid (1+1)
CY 261	Cryptography	3	3	0	CS 112, MATH 233	Face To Face
CY 341	Computer Networks	3	3	0	CS 284	Face To Face
CY 342	Computer Networks Laboratory	1	0	3	CY 341 (or concurrent)	Online (Synchronous)
CY 343	Networks Security	2	2	0	CY 341, CY 261, CY 371	Face To Face
CY 344	Networks Security Laboratory	1	0	3	CY 343 (or concurrent)	Online (Synchronous)
CY 345	Network Defense	2	2	0	CY 344	Face To Face
CY 346	Network Defense Laboratory	1	0	3	CY 345 (or concurrent)	Online (Synchronous)
CY 371	Linux Operating System Laboratory	1	0	3	CS 375	Online (Synchronous)
CY 381	Risk Management	3	3	0	CY 101	Hybrid (1+1)
CY 391	Field Training	3	3	0	Completion of (90 CHs)	Face To Face
CY 411	Reverse Software Engineering	2	0	6	CY 111, CY 101, CY 211	Face To Face
CY 431	Software Security	3	3	0	CY 344, CY 211, CY 452(or concurrent)	Hybrid (1+1)
CY 451	Security Analytics	3	2	3	CY 343, CY 371, CY 111	Face To Face
CY 452	Web Security	3	2	3	CIS 201, CY 343(or concurrent), CIS 221	Face To Face
CY 481	Ethical Hacking (1)	3	1	6	CY 344	Face To Face
CY 482	Ethical Hacking (2)	3	0	9	CY 481, CY 452	Face To Face
CY 483	Digital Forensics	2	2	0	CY 411, CY 451	Hybrid (1+1)
CY 484	Digital Forensics Laboratory	1	0	3	CY 483 (or concurrent)	Online (Synchronous)
CY 491	Cybersecurity Capstone Project (1)	1	1	0	Completion of (90 CHs)	Face To Face
CY 492	Cybersecurity Capstone Project (2)	2	2	0	CY 491	Face To Face

CS 284	Analysis and Design of Algorithms	3	3	0	CS 211	Face To Face
CS 362	Artificial Intelligence	3	3	0	CS 284	Face To Face
CS 375	Operating Systems	3	3	0	CS 211	Face To Face
CIS 201	Introduction to Web Design	1	0	3	SE 112	Face To Face
CIS 203	Communication and Professional Ethics	2	2	0	-	Hybrid (1+1)
CIS 332	Systems Analysis and Design	3	3	0	CIS 221	Face To Face
MATH. 140	Elements Of Linear Algebra	3	3	0	-	Face To Face
MATH 233	Probability & Statistics ( <i>for computer science students</i> )	3	3	0	MATH 102	Face To Face

### **3-a) Department Elective Requirements (12 CH):**

Chosen by the student from the below list of courses, provided that at least **9 CHs** of them are from the Department of Cybersecurity\*.

**Table (4):** Elective Department

Course Number	Course Title	Credit Hours	Weekly Hours		Prerequisite	Teaching Mode
			Lecture	Lab		
CY 321	Database Security	3	2	3	CY 261, CIS 221	Hybrid (1+1)
CY 412	Mobile App Development	3	0	9	SE 112	Face To Face
CY 453	Cloud Computing Security	3	3	0	CY 452	Hybrid (1+1)
CY 454	IoT security	3	3	0	CY 343	Hybrid (1+1)
CY 455	Healthcare security and privacy	3	3	0	CY 101	Hybrid (1+1)
CY 456	Deep Learning	3	3	0	CS 362	Face To Face
CY 461	Introduction to Steganography	3	2	3	CY 261	Hybrid (1+1)
CY 462	Advanced Cryptography	3	3	0	CY 261	Face To Face
CY 471	Operating Systems Security	3	2	3	CY 371, CY 261	Face To Face
CY 485	Formal methods for cybersecurity	3	3	0	CY 261	Face To Face
CY 493-A	Special Topic in Cybersecurity (1)	3	3	0	Department Approval	Online (Synchronous)
CY 493-B	Special Topic in Cybersecurity (2)	3	3	0	Department Approval	Online (Synchronous)
-	A course from other IT departments (400 Level or above )	3	3	0	Department Approval	Face To Face

\*The student is exempt from studying 3 CHs from the optional courses if s/he joins one of the international academies specialized in offering technical courses or joins a technical training course offered in the college in which the number of training hours exceeds 150 hours, provided that s/he obtains an internationally accredited certificate for that course.

## Recommended Study Plan

### 1<sup>st</sup> Year

<b>Semester 1</b>			
Course Number	Course Name	Credits Hours	Prerequisite
MATH 101	Calculus I	3	-
MATH 241	Discrete Mathematics	3	-
CS 101	Introduction to Programming	3	CIS 99 ( <i>or concurrent</i> )
CS 101	Introduction to Programming (Practical)	0	CS 101 ( <i>or concurrent</i> )
LG 101	Communication Skills in English	3	Passing ENG 099
HSS 110	Leader And Social Responsibility	3	-
SE 103	Introduction to Information Technology	3	CS 101 ( <i>or concurrent</i> )
<b>Total</b>		<b>18</b>	
<b>Semester 2</b>			
Course Number	Course Name	Credits Hours	Prerequisite
CY 101	Cybersecurity Fundamentals	3	CS 101
SE 112	Introduction to Object-Oriented programming	3	Pass CS 102
SE 112	Object-Oriented Programming Lab	0	<i>concurrent with SE 112</i>
MATH 102	Calculus (2)	3	<i>MATH 101</i>
MATH 140	Elements Of Linear Algebra	3	-
LG 103	Life Skills	2	-
CY 111	Assembly Language Laboratory	1	SE 112 ( <i>or concurrent</i> )
<b>Total</b>		<b>15</b>	



## 2<sup>nd</sup> Year

<b>Semester 1</b>			
<b>Course Number</b>	<b>Course Name</b>	<b>Credits Hours</b>	<b>Prerequisite</b>
ARB 102	Communication Skills in Arabic	3	-
CY 211	Selected Visual Programming Language	3	SE 112
Math 233	Probability & statistics ( <i>for computer science students</i> )	3	Math 102
CS 211	Data Structures	2	Pass SE 112 + MATH 241
CIS 201	Introduction to Web Design	1	<i>SE 112</i>
CIS 203	Communication and Professional Ethics	2	-
	University Elective	3	
<b>Total</b>		<b>17</b>	
<b>Semester 2</b>			
<b>Course Number</b>	<b>Course Name</b>	<b>Credits Hours</b>	<b>Prerequisite</b>
CIS 221	Fundamentals of Database Systems	3	CS 211
CY 201	Cybersecurity Ethics	1	CY 101
CS 284	Analysis and Design of Algorithms	3	CS 211
CS 375	Operating Systems	3	CS 211
CY 261	Cryptography	3	CS 112, MATH 233
HSS 119	Entrepreneurship And Innovation	2	-
-	University Elective	3	-
<b>Total</b>		<b>18</b>	

### 3<sup>rd</sup> Year

Semester 1			
Course Number	Course Name	Credits Hours	Prerequisite
MS 100	Military Sciences	3	-
CIS 332	Systems analysis and design	3	CIS 221
CY 341	Computer Networks	3	CS 284
CY 371	Linux Operating System laboratory	1	CS 375
CY 342	Computer Networks Laboratory	1	CY 341 ( <i>or concurrent</i> )
CS 362	Artificial Intelligence	3	CS 284
	Department Elective (1)	3	
<b>Total</b>		<b>17</b>	
Semester 2			
Course Number	Course Name	Credits Hours	Prerequisite
CY 343	Networks Security	2	CY 341, CY 261, CY 371
CY 381	Risk Management	3	CY 101
CY 411	Reverse Software Engineering	2	CY 111, CY 101, CY 211
CY 344	Networks Security Laboratory	1	CY 343 ( <i>or concurrent</i> )
CY 452	Web Security	3	CIS 201, CY 343( <i>or concurrent</i> ), CIS 221
	University Elective	3	-
	Department Elective	3	-
<b>Total</b>		<b>17</b>	
Summer			
Course Number	Course Name	Credits Hours	Prerequisite
CY 391	Field Training	3	Completion 90 CHs
<b>Total</b>		<b>3</b>	

**4<sup>th</sup> Year**

<b>Semester 1</b>			
<b>Course Number</b>	<b>Course Name</b>	<b>Credits Hours</b>	<b>Prerequisite</b>
CY 345	Network Defense	2	CY 344
CY 431	Software Security	3	CY 344, CY 211, CY 452 <i>(or concurrent)</i>
CY 346	Network Defense Laboratory	1	CY 345 <i>(or concurrent)</i>
CY 451	Security Analytics	3	CY 343, CY 371, CY 111
CY 481	Ethical Hacking (1)	3	CY 344
-	Department Elective	3	-
CY 491	Cybersecurity Capstone Project (1)	1	Completion of (90 CHs)
<b>Total</b>		<b>16</b>	
<b>Semester 2</b>			
<b>Course Number</b>	<b>Course Name</b>	<b>Credits Hours</b>	<b>Prerequisite</b>
CY 482	Ethical Hacking (2)	3	CY 481, CY 452
CY 483	Digital Forensics	2	CY 411, CY 451
CY 484	Digital Forensics Laboratory	1	CY483 <i>(or concurrent)</i>
CY 492	Cybersecurity Capstone Project (2)	2	CY 491
-	Department Elective	3	-
<b>Total</b>		<b>11</b>	

# Cybersecurity Description of Courses 2021

## **CY 101 Cybersecurity Fundamentals**

**(3C,3T,0L)**

*Prerequisite: CS 101*

This course covers an introduction about classic security topics, such as applied cryptography, authentication, access controls, intrusion prevention and detection, database security, web security, systems security and malware. Moreover, it covers topics related to ethics and laws in cybersecurity.

## **CY 111 Assembly Language Laboratory**

**(1C,0T,3L)**

*Prerequisite: CS 112 (or concurrent)*

This course emphasizes the organization and operation of computer systems at the assembly-language level. Covers mapping of statements and constructs in a high-level language onto sequences of machine instructions, as well as the internal representation of simple data types and structures. Offers programming practice with an assembly language to provide practical application of concepts presented in class.

## **CY 201 Cybersecurity Ethics**

**(1C,1T,0L)**

*Prerequisite: CY 101*

This course introduces the ethical issues in cybersecurity. The coverage includes the definition of ethics, major ethical stances, professional responsibility, fair information practices, codes of ethics, ethical issues in disclosing vulnerabilities, and ethics relation to law. It also includes the presentation and analysis of the dominant ethical frameworks and normative theories.

## **CY 211 Selected Visual Programming Language**

**(2C,0T,6L)**

*Prerequisite: CS 112*

This course covers the fundamentals of GUI, event-driven programming principles, objects and properties, menus, procedures, control structures, and database file processing. Moreover, it explains how to use and implement the components for GUI, such as Buttons and TextBoxes, in an Integrated Development Environment (IDE).

## **CY 261 Cryptography**

**(3C,3T,0L)**

*Prerequisite: CS 112, MATH 233*

This course covers basic concepts in cryptography including encryption/decryption, sender authentication, data integrity, non-repudiation, attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext), symmetric cryptography (i.e. DES and AES) and asymmetric cryptography (i.e. RSA), information-theoretic security (one-time pad, Shannon Theorem), key exchange and digital signatures.

## **CY 321 Database Security**

**(3C,2T,3L)**

*Prerequisite: CY 261, CIS 221*

This course provides an overview of database security concepts and techniques. It covers database security models, access control and its application to database security, multilevel secure relational model, authentication, trust management, privacy protection, and data auditing. The course should also include identifying risks, threats, and vulnerabilities in database systems. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.

**CY 341 Computer Networks****(3C,3T,0L)***Prerequisite: CS 284*

This course covers topics about network architectures, application layer protocols such as HTTP and FTP, transmission layer protocols such as TCP and UDP, network Layer services such as routing protocols, IPV4 and IPV6, data link layer services such as error detection and correction, multiple access control and principles of wireless networks.

**CY 342 Computer Networks Laboratory****(1C,0T,3L)***Prerequisite: CY 341 (or concurrent)*

This laboratory consists of experiments to design, apply, analyze, and evaluate computer network protocols. Moreover, it contains experiments for evaluation static and dynamic routing protocols: RIP, OSPF, and BGP. In addition, the experiments evaluate and analyze TCP and UDP protocols, and focus on DHCP and NAT configuration, and analyze network traffic using sniffing tools.

**CY 343 Networks Security****(2C,2T,0L)***Prerequisite: CY 341, CY 261, CY 371*

This course covers principles and techniques for network and communication security. Basically, it explains many network attacks such as DoS and DDoS, MAC flooding and DHCP spoofing. In addition, the course covers different types of networks countermeasures such as firewalls and NIDS that are used prevent and detect network attacks. Moreover, the course discusses in details how security protocols such as SSL/TLS, SSH and IPsec work.

**CY 344 Networks Security Laboratory****(1C,0T,3L)***Prerequisite: CY 343 (or concurrent)*

This course consists of a set of laboratory experiments security protocols such as SSL/TLS, SSH and IPsec. Moreover, it consists of experiments about conducting attacks against network protocols such as TCP, UDP and ARP, traffic sniffing attacks, DNS hacking, SYN flooding, port scanning, access control, intrusion detection systems, and Firewalls.

**CY 345 Network Defense****(2C,2T,0L)***Prerequisite: CY 344*

This course provides an essential study of network defense, related vulnerability and security issues, and common tools available for network packet analysis and exploitations. Topics to be covered include review of basic concepts and principles related to network defense (networking protocols and cryptography, mission assurance, network policy development and enforcement, etc.), secure network development (network access control, network hardening, implementing firewalls, VPNs, etc.), and advanced network defense techniques (honeypots, honeynets, network monitoring, implementing IDS/IPS, etc.)

**CY 346 Network Defense Laboratory****(1C,0T,3L)***Prerequisite: CY 345 (or concurrent)*

This laboratory is a practical course which covers network and system security topics. The lessons include full practical setup guides, such as labs from Palo Alto for the student to practice their new skills deploying technologies and strategies in a production network. The primary sections of the course are divided up into network security and endpoint security. Network security will teach you secure network design concepts, configuration of network appliances such as switches, and a look into the secure configuration of firewalls, web filtering and advanced malware protection. The endpoint security section focuses mainly on Windows security, as most corporate networks have a majority of Windows systems. You will also learn Active Directory, Group Policy, patch management, endpoint hardening and the vulnerability management cycle. These topics are taught in a practical manner with step-by-step guides on deploying the actual technology in use. Students will leave this course knowing exactly how to accomplish these tasks.

**CY 371 Linux Operating System Laboratory (1C,0T,3L)**

*Prerequisite: CS 375*

This course covers some topics of Linux operating system, such as file system, commands, utilities, text editing, shell programming and text processing utilities.

**CY 381 Risk Management (3C,3T,0L)**

*Prerequisite: CY 101*

This course discusses how to find and control risks in information assets using risk identification, assessment and analysis, and control approaches. Moreover, it covers malicious human behavioral factors that harm information systems.

**CIS 391: Field Training (3C, 3T,0L)**

*Prerequisite: Completion of 90 credit hours*

This course provides students with the chance to experience the work environment before graduation. Students are required to spend a predetermined work period as an intern in an institution approved by the CY department. During this period, students need to get engaged in cybersecurity practices with their mentors and observe and experience the cybersecurity roles in these institutions.

**CY 411 Reverse Software Engineering (2C,0T,6L)**

*Prerequisite: CY 111, CY 101, CY 211*

The object of Software Reverse Engineering is to provide students with the understanding and practice to perform analysis on malware, deduce their and determine how malware works, and to aid the analysis via disassembly. Students will be able to use tools (IDAPro, Ollydbg) to safely perform static and dynamic analysis of malware, including encoded, packed, obfuscated ones. In particular, the course will have extensive hands-on labs/assignments on each knowledge unit.

**CY 412 Mobile App Development (3C,0T,9L)**

*Prerequisite: CS 112*

Mobile computing devices have become ubiquitous. This course focuses on the development of mobile solutions for various modern platforms, including major mobile operating systems such as Android and iOS. The course covers different topics such as mobile device architecture, programming languages, software engineering, user interface design, RESTful and Non-RESTful apps, creating and incorporating Web/Cloud Services, mobile Sensors and security and trust management.

**CY 431 Software Security (3C,3T,0L)**

*Prerequisite: CY 344, CY 211, CY 452(or concurrent)*

Theory and practice of software security, focusing in particular on some common software security risks, including buffer overflows, race conditions and random number generation, and on identification of potential threats and vulnerabilities early in design cycle. Emphasizes methodologies and tools for identifying and eliminating security vulnerabilities, techniques to prove absence of vulnerabilities, ways to avoid security holes in new software, and essential guidelines for building secure software: how to design software with security in mind from the ground up and to integrate analysis and risk management throughout the software life cycle.

**CY 451 Security Analytics****(3C,2T,3L)***Prerequisite: CY 343, CY 371, CY 111*

This course aims at monitoring and documentation networks, locking down networks, thwart malware, prevent hacks by improving visibility into the environment, using the power of data and security. In addition, the course covers topics such as how to monitor computer networks, acquire and prepare security data, correlate security events, use simple statistical methods to detect malware and predict rogue behavior. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.

**CY 452 Web Security****(3C,2T,3L)***Prerequisite: CIS 201, CY 343(or concurrent), CIS 221*

This course introduces you to the field of web security: that is, how to build secure web applications. The course covers fundamental concepts of web programming, web vulnerability exploitation, web browser design flaws, and a few advanced topics in web privacy and E-commerce Security. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.

**CY 453 Cloud Computing Security****(3C,3T,0L)***Prerequisite: CY 452*

The course will describe the Cloud security architecture and explore the guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver and manage secure cloud based services. The course delves deep into the secure cloud architectural aspects with regards to identifying and mitigating risks, protection and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. The course will leverage cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA).

**CY 454 IoT Security****(3C,3T,0L)***Prerequisite: CY 343*

This course covers the basic components of IoT and how data is collected and analyzed from sensors. Moreover, this course discusses the security issues and solutions of internet of things, and explains different threats to IoT platforms and teaches students how to defend IoT devices securely.

**CY 455 Healthcare Security and Privacy****(3C,3T,0L)***Prerequisite: CY 101*

This course covers several concepts such as, an introduction to privacy and security of healthcare information systems, how to protect the confidentiality of patient information, types of access and the appropriate availability of healthcare information to healthcare providers, concepts of limiting unauthorized access, standards and specifications that help keeping patient medical information secure in an electronic environment, common data protection issues, and exchanging clinical information between healthcare organizations need to be addressed. Related case studies will be used and administrative issues will be researched and presented by students as the course project.

**CY 456 Deep Learning****(3C,3T,0L)***Prerequisite: CS 362*

This course will cover main concepts and principles in deep learning. It covers word vector representations, window-based neural networks, recurrent neural networks, long-short-term memory models, recursive neural networks, convolutional neural networks as well as some recent models involving a memory component. The course provides a thorough introduction to cutting-edge research in deep learning applied to pattern recognition, speech recognition, and natural language processing and understanding.

**CY 461 Introduction to Steganography****(3C,2T,3L)***Prerequisite: CY 261*

This course introduces the fundamentals of steganography. It covers the concepts of digital steganography, digital steganalysis, and digital watermarking including hiding algorithms on different carrier files (image, audio, and video files). The course includes an introduction to well-known tools to both hide and extract information. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.

**CY 462 Advanced Cryptography****(3C,3T,0L)***Prerequisite: CY 261*

This course covers advanced topics in cryptography such as advanced protocols (i.e. Zero-knowledge proofs, and protocols, Secret sharing), fully homomorphic encryption, obfuscation and quantum cryptography.

**CY 471 Operating Systems Security****(3C,2T,3L)***Prerequisite: CY 371, CY 261*

This course introduces the fundamentals of operating systems (OS) security. The coverage includes access control mechanisms, memory protections, and OS-level mechanisms (hardware and software) and policies to protect against attacks and threats such as rootkits and malware. The course also includes the concepts of virtual machines and their use to understand and analyze modern OSs (including mobile OSs) in order to identify OS-related risks, threats, and vulnerabilities. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.

**CY 481 Ethical Hacking (1)****(3C,1T,6L)***Prerequisite: CY 344*

This course introduces the ethics and laws of ethical hacking, and it discusses the different types of threats including insider threat. Moreover, it explains the approaches that an ethical hacker uses for footprinting and reconnaissance, scanning networks, enumeration, vulnerability analysis and system hacking. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in ethical hacking.

**CY 482 Ethical Hacking (2)****(3C,0T,9L)***Prerequisite: CY 481, CY 452*

This course discusses advanced topics in ethical hacking, and consists of advanced laboratory experiments such as malware threats and analysis, sniffing, social engineering, denial of service, session hijacking, evading security countermeasures, hacking web servers and applications, SQL injection, hacking wireless networks, hacking mobile platforms and IoT hacking. Furthermore, this course consists of a set of laboratory experiments that provides hands-on experience in this topic.



**CY 483 Digital Forensics (2C,2T,0L)**

*Prerequisite: CY 411, CY 451*

This course introduces a theoretical and practical knowledge on the principles and practices of digital forensics. It covers the sources of digital evidence, digital investigation, and fundamentals of computer forensics. Coverage includes disk examination, memory acquisition, and logging analysis. The course also includes registry, e-mail, and database forensics.

**CY 484 Digital Forensics Laboratory (1C,0T,3L)**

*Prerequisite: CY 483 (or concurrent)*

This course gives a practical hands-on experience on a selected set of state-of-the-art common forensic tools (open-source or proprietary). The coverage includes the introduction to the functionalities, underlying theory, and contrasting of such tools.

**CY 485 Formal Methods for Cybersecurity (3C,3T,0L)**

*Prerequisite: CY 261*

This course introduces the application of formal methods to cybersecurity. It focuses on the formal specification of security protocols using mathematically defined languages such as SPS, AVISPA-IF, and  $\pi$ -calculus, then formally verify specified protocols using state-of-the-art automated techniques and tools such as OFMC model checker, and Proverif static analyzer.

**CY 491 Cybersecurity Capstone Project (1) (1C, 0T, 0L)**

*Prerequisite: Completion of 90 credit hours*

In this course the student implements, tests and presents the proposed system or software to a 3-member faculty committee including the project supervisor.

**CY 492 Cybersecurity Capstone Project (2) (2C, 0T, 0L)**

*Prerequisite: CY 491*

This is a continuation of CY 491, where the student implements, tests and presents the proposed system or software to a 3-member faculty committee that includes the project's supervisor. A written report is to be submitted to the department and committee.

**CY 493-A Special Topics in Cybersecurity (1) (3C, 0T, 0L)**

*Prerequisite: Department Approval*

The department chooses a topic related to the field of cybersecurity.

**CY 493-B Special Topics in Cybersecurity (2) (3C, 0T, 0T)**

*Prerequisite: Department Approval*

The department chooses a topic related to the field of cybersecurity.