

جامعة الفلوجة
University of Fallujah



***First Cycle – Bachelor's Degree (B.Sc.)
Cybersecurity (2025-2026)***



Table of Contents

1. Overview
 2. Undergraduate Modules 2025-2026
 3. Contact
-

1. Overview

This guide provides an overview of the academic courses offered within the Bachelor of Science (B.Sc.) program in Cybersecurity. The program consists of 40 academic courses with a total student workload of 6,000 hours and 240 ECTS credits, delivered in accordance with the principles and requirements of the Bologna Process.

The curriculum is designed to provide students with a comprehensive and progressive education in cybersecurity, beginning with the fundamental disciplines of computer science and gradually advancing toward specialized cybersecurity domains. Students first develop strong foundations in mathematics, programming, computer networks, operating systems, algorithms, data structures, digital logic, databases, and web technologies. These foundations are subsequently extended through advanced study in cryptography, network security, software security, secure communication protocols, penetration testing, digital forensics, malware analysis, cloud computing, artificial intelligence for cybersecurity, and related fields.

The curriculum emphasizes a balanced combination of theoretical knowledge, practical laboratory experience, and hands-on technical skills. Through extensive laboratory work, projects, and applied learning activities, students gain experience with modern cybersecurity tools, platforms, and technologies used in professional environments.

The program is designed to prepare graduates for a wide range of professional and academic pathways, including software development, network administration, cybersecurity operations, ethical hacking, penetration testing, digital forensics, security analysis, systems administration, cybersecurity consulting, and postgraduate studies and research.

To facilitate course identification and classification, each course is assigned a unique course code. The course code consists of the department prefix (CYS) followed by a three-digit number. The first digit indicates the academic level (year of study), while the last digit identifies the course category as follows:

Final Digit	Course Category
1	Programming and Software Development
2	Reserved for Future Use
3	Mathematics and Theoretical Foundations

4	Professional Practice and Research
5	Core Computer Science
6	Artificial Intelligence and Emerging Technologies
7	Networks and Communication Systems
8	Cybersecurity, System Security, Digital Forensics, and Penetration Testing
9	Cryptography and Cryptanalysis

This classification system provides a clear structure for organizing courses and reflects the multidisciplinary nature of the cybersecurity curriculum.

2. Undergraduate Courses 2025-2026

First Year

Module 1

Code	Course/Module Title	ECTS	Semester
CYS101	Structured Programming I	8	1
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)
3	2	78	122
Description			
Structured Programming I introduces the fundamental concepts of computer programming and algorithmic problem-solving using the structured programming paradigm. The course develops students' ability to analyze problems, design logical solutions, and implement programs using the C++ programming language. Topics include program structure, syntax and semantics, data types, input and output operations, control structures, functions, arrays, and basic modular programming techniques. Emphasis is placed on writing clear, efficient, and well-structured code while developing foundational computational thinking and software development skills essential for advanced computing and cybersecurity studies.			

Module 2

Code	Course/Module Title	ECTS	Semester
CYS133	Discrete Mathematics	6	1
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL

			(hr/sem)
2	2	78	72
Description			
Discrete Mathematics introduces the fundamental mathematical structures and reasoning techniques that underpin computer science and cybersecurity. The course develops students' analytical and logical thinking skills through the study of propositional and predicate logic, sets, relations, functions, recursion, counting principles, and matrix operations. It also explores essential discrete structures such as graphs, trees, and binary trees, which are widely used in algorithms, data structures, networks, and secure computing applications. In addition, the course introduces coding systems and formal mathematical methods that support problem-solving and computational modeling in modern computing environments.			

Module 3

Code	Course/Module Title	ECTS	Semester
CYS109	Data Security Principles	5	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/sem)
3	0	48	77
Description			
Data Security Principles introduces the fundamental concepts and techniques used to protect information and ensure secure communication in digital systems. The course examines the core principles of data confidentiality, integrity, and secure data processing through the study of classical and modern cryptographic methods. Topics include simple substitution and transposition ciphers, modular arithmetic, stream ciphers, pseudorandom sequence generation using Linear Feedback Shift Registers (LFSRs), and block cipher design principles with emphasis on the Data Encryption Standard (DES) algorithm. The course also explores the mathematical foundations of cryptography and develops students' understanding of how encryption techniques are applied to secure information in modern computing and cybersecurity environments.			

Module 4

Code	Course/Module Title	ECTS	Semester
CYS103	Mathematics	7	1
Class (hr/w)	Tut (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)
3	2	78	97
Description			
Mathematics provides the fundamental mathematical knowledge and analytical skills			

required for computer science and cybersecurity studies. The course introduces essential topics in algebra, functions, calculus, matrices, and introductory differential equations, with emphasis on problem-solving and quantitative reasoning. Students develop the ability to analyze mathematical problems, perform logical and numerical computations, and apply mathematical techniques to computing, engineering, and information technology applications. The course strengthens the mathematical foundation necessary for advanced subjects such as algorithms, cryptography, data analysis, and secure system design.

Module 5

Code	Course/Module Title	ECTS	Semester
UFall111	English language I	2	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/sem)
2	0	32	18
Description			
This course is designed to enhance students' proficiency in the English language, focusing on academic and scientific communication. Topics include grammar, vocabulary, reading comprehension, writing skills, and oral communication. The course aims to develop the language skills necessary for effective communication in the field of Cybersecurity and other scientific disciplines.			

Module 6

Code	Course/Module Title	ECTS	Semester
UFall113	Democracy and Human Rights	2	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/sem)
2	0	32	18
Description			
The aim of the "Human Rights and Democracy" module is to provide a comprehensive understanding of the principles, institutions, and challenges related to human rights and democratic governance, emphasizing their interdependence and relevance in contemporary societies.			

Module 7

Code	Course/Module Title	ECTS	Semester
CYS111	Structured Programming II	8	2
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)

3	2	78	122
Description			
Structured Programming II builds upon the foundations established in Structured Programming I by advancing students' programming, problem-solving, and software development skills using C++. The course introduces more advanced programming concepts, including modular design, recursion, file handling, pointers, dynamic memory management, and structured data processing. It also provides an introduction to object-oriented programming principles such as classes, objects, encapsulation, inheritance, and polymorphism. Emphasis is placed on developing efficient, maintainable, and reusable software solutions while strengthening analytical thinking and practical programming proficiency for more advanced computing and cybersecurity applications.			

Module 8

Code	Course/Module Title	ECTS	Semester
CYS107	Computer Networks Fundamentals	6	2
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)
3	2	78	72
Description			
Computer Networks Fundamentals introduces the fundamental principles of data communication and computer networking. The course covers communication systems, network components, protocols, standards, and different types of network connectivity. Students study the OSI model and Internet networking models, with detailed examination of their layers and functions. Topics include digital and analog signals, data transmission, error detection and correction, framing, addressing, routing concepts, routing algorithms, transport layer protocols, congestion control, and quality of service. The course also introduces network media, cable types, routers, switches, and basic network setup techniques. Practical laboratory activities using network simulation tools such as Cisco Packet Tracer are integrated throughout the course to develop foundational skills in network configuration, connectivity, and troubleshooting. Emphasis is placed on understanding how modern computer networks operate and how communication protocols support reliable and secure data exchange.			

Module 9

Code	Course/Module Title	ECTS	Semester
CYS108	Cybersecurity Fundamentals	7	2
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)
3	2	78	97

Description
Cybersecurity Fundamentals introduces the essential concepts and practices used to protect computer systems, networks, and digital information from security threats and unauthorized access. The course provides foundational knowledge in information security principles, including confidentiality, integrity, authentication, and access control. Students are introduced to operating system fundamentals, virtualization, command-line environments, basic networking, password security, network scanning, packet analysis, and common cybersecurity tools and techniques. The course also explores fundamental attack and defense concepts, including monitoring, traffic interception, and Man-in-the-Middle (MITM) attacks, with emphasis on understanding how cyber threats operate and how secure practices can mitigate them. Practical laboratory activities are integrated throughout the course to develop hands-on technical and analytical skills essential for advanced cybersecurity studies.

Module 10

Code	Course/Module Title	ECTS	Semester
CYS105	Digital Logic Design	5	2
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/sem)
2	2	63	62
Description			
Digital Logic Design introduces the fundamental principles of digital systems and electronic logic that underpin modern computing and cybersecurity technologies. The course covers number systems, data representation, Boolean algebra, logic gates, combinational and sequential circuits, flip-flops, counters, registers, multiplexers, and memory components. It also introduces finite state machines and basic processor organization to develop an understanding of how digital hardware systems operate. In the context of cybersecurity, the course highlights the role of secure hardware design, trusted computing, hardware-based access control, and the fundamentals of cryptographic hardware and embedded system security. Emphasis is placed on analyzing and designing reliable digital circuits that support secure and efficient computing systems.			

Module 11

Code	Course/Module Title	ECTS	Semester
CYS113	Probability and Statistic	2	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/sem)
2	0	32	18
Description			

Probability and Statistics introduces the fundamental concepts and methods used for data analysis, probabilistic modeling, and statistical reasoning in computing and cybersecurity applications. The course covers data organization and presentation, frequency distributions, graphical analysis, measures of central tendency and variation, correlation, and regression. It also introduces probability theory, counting techniques, conditional probability, and Bayes' theorem. Students study discrete and continuous probability distributions, including binomial, Poisson, uniform, normal, and exponential distributions, in addition to sampling, estimation, and hypothesis testing. Emphasis is placed on developing analytical and quantitative skills for interpreting data, evaluating uncertainty, and supporting decision-making in scientific and technological contexts.

Module 12

Code	Course/Module Title	ECTS	Semester
UFall120	Arabic language I	2	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	32	18
Description			
The course covers fundamental aspects of the Arabic language, focusing on both written and spoken forms. Students often learn basic grammar, vocabulary, pronunciation, and writing skills. As well as teaching students the method of analyzing the literary text by referring to significant literary texts.			

Second Year

Module 13

Code	Course/Module Title	ECTS	Semester
CYS201	Object Oriented Programming I	5	3
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	47
Description			
Object-Oriented Programming I introduces the fundamental concepts of object-oriented programming using the Python programming language. The course focuses on problem-solving, program design, and the development of reusable and maintainable software through object-oriented principles. Topics include classes, objects, methods, encapsulation, inheritance, polymorphism, file handling, exception handling, and basic data structures. Students also develop practical programming skills through laboratory exercises and small software projects, with introductory exposure to security-related programming concepts and selected Python libraries relevant to cybersecurity applications.			

Module 14

Code	Course/Module Title	ECTS	Semester
CYS205	Data Structures	5	3
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Object-Oriented Programming I introduces the fundamental concepts of object-oriented programming using the Python programming language. The course focuses on problem-solving, program design, and the development of reusable and maintainable software through object-oriented principles. Topics include classes, objects, methods, encapsulation, inheritance, polymorphism, file handling, exception handling, and basic data structures. Students also develop practical programming skills through laboratory exercises and small software projects, with introductory exposure to security-related programming concepts and selected Python libraries relevant to cybersecurity applications.			

Module 15

Code	Course/Module Title	ECTS	Semester
CYS217	Computer Networks	6	3
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Computer Networks builds upon the foundational concepts introduced in Computer Networks Fundamentals and provides a deeper study of modern network technologies, architectures, and protocols. The course examines advanced networking concepts including IP addressing and subnetting, switching, routing, wireless networks, network services, transport protocols, and network management. Emphasis is placed on the configuration, operation, troubleshooting, and performance analysis of computer networks through extensive practical and hands-on laboratory activities. Students gain experience using networking tools, simulators, and real network devices to develop practical skills in network implementation and administration. The course also establishes the technical foundation required for advanced studies in Network Security and secure communication systems.			

Module 16

Code	Course/Module Title	ECTS	Semester
CYC229	Cryptography	6	3
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			

Cryptography builds upon the foundations established in Data Security Principles and provides an in-depth study of modern symmetric cryptographic systems and secure data protection techniques. As a high-ECTS course, it covers the theoretical foundations, practical implementation, and security analysis of major symmetric encryption algorithms and stream ciphers. Topics include classical cryptographic concepts, pseudorandom sequence generation, stream ciphers, block cipher structures, encryption modes of operation, lightweight cryptography, and detailed study of core algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), RC4, and ChaCha20. The course also introduces fundamental cryptanalysis techniques and examines the strengths, weaknesses, implementation risks, and security limitations of different cryptographic approaches. Emphasis is placed on practical laboratory work and hands-on implementation exercises that enable students to develop, analyze, and compare cryptographic algorithms in real computing environments. The course establishes the theoretical and practical foundation required for subsequent study in Advanced Cryptography, which focuses on public-key cryptography and advanced cryptographic protocols.

Module 17

Code	Course/Module Title	ECTS	Semester
CYS231	Web Design	4	3
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	37
Description			
Web Design introduces the fundamental concepts and technologies used in the development of modern websites and web interfaces. The course covers client-server architecture, web communication fundamentals, HTTP requests and methods, and the structure of web applications. Students learn the basics of HTML and CSS for creating and styling web pages, including layouts, navigation structures, forms, and responsive design principles. Emphasis is placed on practical laboratory work and hands-on activities that enable students to design, implement, and test interactive web pages and basic web interfaces. Through practical exercises and mini-projects, students develop foundational skills in front-end web development and gain the necessary background for subsequent courses in web application development and secure web technologies.			

Module 18

Code	Course/Module Title	ECTS	Semester
UFall225	English language II	2	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	32	18
Description			
English Language II builds upon the language skills developed in English Language I and focuses on enhancing students' proficiency in academic and professional communication.			

The course develops advanced reading, writing, listening, and speaking skills through the study of academic texts, technical materials, and discipline-related topics. Students improve their ability to write reports, summaries, presentations, and professional correspondence while expanding their vocabulary and grammatical accuracy. Special emphasis is placed on academic writing, critical reading, oral communication, and the use of English in scientific, technological, and cybersecurity contexts. The course aims to strengthen students' ability to communicate effectively in academic, professional, and multicultural environments and to engage with technical literature throughout their studies and future careers.

Module 19

Code	Course/Module Title	ECTS	Semester
UFall211	Ba'ath Regime Crimes	2	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	32	18
Description			
Ba'ath Regime Crimes in Iraq introduces students to the major legal, political, and human rights violations committed during the rule of the Ba'ath regime in Iraq. The course examines key historical events, relevant legal frameworks, decisions of the Iraqi High Criminal Court, and the social and institutional impacts of these crimes. Emphasis is placed on promoting legal awareness, respect for human rights, and understanding the principles of justice and accountability within the Iraqi context.			

Module 20

Code	Course/Module Title	ECTS	Semester
CYS211	Object Oriented Programming II	5	4
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	47
Description			
Object-Oriented Programming II builds upon the concepts introduced in Object-Oriented Programming I by exploring advanced object-oriented design and software development techniques using Python. The course covers advanced data structures, modular programming, graphical interfaces, multithreading, networking fundamentals, and software development practices for larger applications. A significant practical component of the course is dedicated to introducing students to cybersecurity and cryptographic libraries in Python, including their implementation, usage, and integration into security-focused applications. Through hands-on laboratories and practical projects, students gain experience in developing secure and efficient Python-based solutions for cybersecurity and information security tasks.			

Module 21

Code	Course/Module Title	ECTS	Semester
------	---------------------	------	----------

CYS225	Analysis & Design of Algorithms	5	4
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	47
Description			
Analysis and Design of Algorithms introduces the fundamental principles and techniques used to design, analyze, and optimize computer algorithms. The course covers algorithmic strategies such as brute force, divide and conquer, greedy methods, dynamic programming, recursion, and graph-based algorithms, with emphasis on computational efficiency and complexity analysis using time and space evaluation methods. Students learn how to compare algorithm performance, analyze correctness, and develop efficient solutions for computational problems. The course also includes practical laboratory activities and hands-on programming exercises that strengthen problem-solving and algorithm implementation skills. In the final part of the course, selected topics focus on the design and analysis of algorithms used in cybersecurity and secure computing applications, including cryptographic and security-related algorithmic concepts.			

Module 22

Code	Course/Module Title	ECTS	Semester
CYS261	Web Application Development	5	4
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Web Application Development I builds upon the foundations introduced in Web Design and focuses on the development of dynamic and database-driven web applications. The course covers server-side programming using PHP and database integration using MySQL. Students learn how to design and implement custom web applications, manage user input, process forms, handle sessions, and interact with databases in client-server environments. The course also introduces secure web development practices and examines common web application vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), insecure authentication, and improper input validation. Strong emphasis is placed on heavy laboratory work and hands-on practical development activities that enable students to build, test, and secure real web applications.			

Module 23

Code	Course/Module Title	ECTS	Semester
CYS213	Computation Theory	4	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
3	0	48	52

Description
Computation Theory introduces the fundamental theoretical concepts that define the capabilities and limitations of computation. The course examines formal models of computation, including finite automata, regular languages, context-free grammars, pushdown automata, and Turing machines. Students study language recognition, computability, decidability, and the mathematical foundations of algorithms and computational processes. The course also explores complexity concepts and the classification of computational problems according to their solvability and resource requirements. Emphasis is placed on developing formal reasoning and analytical skills essential for advanced studies in computer science, cybersecurity, algorithms, and secure system design.

Module 24

Code	Course/Module Title	ECTS	Semester
CYS251	Database Management Systems	5	4
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Database Management Systems introduces the fundamental concepts, models, and technologies used for the design, implementation, and management of modern database systems. The course covers data modeling, entity-relationship diagrams, relational database design, normalization, Structured Query Language (SQL), database transactions, indexing, and database administration concepts. Students learn how to design and develop efficient database applications while understanding data integrity, consistency, and efficient data retrieval techniques. The course includes practical laboratory activities and hands-on exercises focused on database design, query development, and database management using modern database systems. In the final part of the course, students are introduced to database security concepts, including access control, authentication, data protection, backup strategies, common database vulnerabilities, and secure database management practices.			

Module 25

Code	Course/Module Title	ECTS	Semester
CYC258	Software Security	4	4
Class (hr/w)	Lab	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	37
Description			
Software Security introduces the fundamental principles and practices used to develop, analyze, and maintain secure software systems. The course examines common software vulnerabilities, secure coding practices, input validation, authentication mechanisms,			

access control, memory-related vulnerabilities, and software exploitation concepts. Students study the causes and impact of security flaws such as buffer overflows, injection attacks, insecure authentication, improper error handling, and insecure data management. The course also covers secure software development life cycle (SSDLC) concepts, threat modeling, vulnerability assessment, code review, and basic application hardening techniques. Practical laboratory activities and hands-on exercises are integrated throughout the course to develop skills in identifying, analyzing, and mitigating software security weaknesses in real-world applications.

Module 26

Code	Course/Module Title	ECTS	Semester
UFall224	Arabic language II	2	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	32	18
Description			
Arabic Language II builds upon the language skills developed in Arabic Language I and focuses on enhancing students' proficiency in academic and professional communication in Arabic. The course develops advanced reading, writing, and communication skills through the study of literary, academic, and technical texts. Students improve their ability to prepare reports, summaries, presentations, and formal written documents while strengthening their grammatical accuracy and language proficiency. Special emphasis is placed on effective written and oral communication, critical reading, and the use of Arabic in academic and professional contexts. The course aims to strengthen students' ability to communicate clearly and effectively and to engage with scholarly and professional materials throughout their studies and future careers.			

Third Year

Module 27

Code	Course/Module Title	ECTS	Semester
CYS339	Advanced Cryptography	7	5
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	97
Description			
Advanced Cryptography builds upon the concepts introduced in Data Security Principles and Cryptography, and provides an in-depth study of modern public-key cryptographic systems and advanced security protocols. The course focuses on asymmetric cryptography, including public-key encryption, key exchange and key sharing methods, digital signatures, authentication protocols, and cryptographic hashing techniques. Students study the mathematical foundations and operational principles of major public-key algorithms and			

secure communication mechanisms, together with their practical applications in modern cybersecurity systems. The course also introduces fundamental concepts in cryptanalysis and security evaluation, preparing students for more advanced study in cryptographic attacks and analysis. Practical laboratory activities and hands-on implementation exercises are integrated throughout the course to develop skills in implementing, analyzing, and evaluating advanced cryptographic methods and secure communication protocols.

Module 28

Code	Course/Module Title	ECTS	Semester
CYS325	Operating Systems	6	5
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Operating Systems introduces the fundamental concepts, architecture, and functionality of modern operating systems. The course examines process and thread management, memory management, file systems, input/output management, scheduling algorithms, synchronization, deadlocks, and resource allocation techniques. Students study how operating systems manage hardware and software resources while providing secure and efficient execution environments for applications and users. The course also introduces concepts related to user management, permissions, virtualization, and operating system security mechanisms. A strong emphasis is placed on practical and hands-on learning through extensive laboratory activities covering both Microsoft Windows and Linux environments, including server administration and system configuration tasks. Students gain practical experience in command-line environments, process monitoring, system administration, resource management, shell scripting, and basic server deployment and management in modern computing environments.			

Module 29

Code	Course/Module Title	ECTS	Semester
CYS337	Secure Communication Protocols	4	5
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	37
Description			
Secure Communication Protocols builds upon the concepts introduced in computer networks and cryptography courses and focuses on the mechanisms and protocols used to achieve secure data communication in modern networks and distributed systems. The course examines the design, operation, and security properties of communication protocols used for authentication, confidentiality, integrity, and secure key exchange. Topics include secure transport protocols, virtual private networks, wireless security protocols, secure email communication, certificate-based authentication, and cryptographic protocol integration in networked environments. Students also study common protocol			

vulnerabilities, attacks against communication systems, and methods for analyzing and securing protocol implementations. The course includes practical laboratory activities and hands-on exercises focused on configuring, analyzing, monitoring, and evaluating secure communication protocols and encrypted network services in real and simulated networking environments.

Module 30

Code	Course/Module Title	ECTS	Semester
CYS338	Penetration Testing I	6	5
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	3	78	72
Description			
Penetration Testing I builds upon the knowledge and practical skills developed in Cybersecurity Fundamentals and Network Security. As a high-ECTS course, it provides an intensive introduction to penetration testing methodologies, security assessment techniques, and ethical hacking practices used to identify and evaluate vulnerabilities in computer systems and networks. The course covers reconnaissance, scanning, enumeration, vulnerability assessment, exploitation fundamentals, password attacks, web application testing basics, network service analysis, and post-exploitation concepts within controlled and authorized environments. Strong emphasis is placed on extensive laboratory work and hands-on practical activities using modern cybersecurity tools, virtualized environments, and realistic attack scenarios to develop technical, analytical, and reporting skills required for professional security testing and defensive security analysis.			

Module 31

Code	Course/Module Title	ECTS	Semester
CYS391	Open Source Web Development	5	5
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Web Application Development extends the concepts and practical skills developed in Web Application Development by focusing on open-source web development platforms, modern web technologies, and content management systems. The course covers modern web application requirements, API integration, plugin and module development, and customization of open-source platforms such as WordPress and Drupal. Students study the architecture, extension mechanisms, deployment methods, and security considerations associated with large-scale web platforms and modular web development. The course also examines common security issues related to plugins, modules, APIs, authentication systems, and web platform configuration. Extensive laboratory activities and hands-on practical projects are integrated throughout the course to develop professional skills in modern web application development, integration, deployment, and security assessment.			

--

Module 32

Code	Course/Module Title	ECTS	Semester
CYS304	Hacking Ethics and Laws	2	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	33	17
Description			
Hacking Ethics and Laws examines the ethical, legal, and professional responsibilities associated with cybersecurity practices and offensive security activities. The course introduces students to cybercrime laws, digital privacy regulations, intellectual property rights, ethical hacking standards, responsible disclosure practices, and legal considerations related to penetration testing and security research. Students study real-world cybersecurity incidents, professional codes of ethics, cyber warfare concerns, digital evidence handling, and the societal impact of cyber operations and emerging technologies. The course also explores legal frameworks governing computer misuse, unauthorized access, data protection, and cyber investigations at both national and international levels. Emphasis is placed on ethical decision-making, professional conduct, and understanding the legal boundaries and responsibilities of cybersecurity professionals.			

Module 33

Code	Course/Module Title	ECTS	Semester
CYS349	Cryptanalysis	6	6
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Cryptanalysis builds upon the knowledge gained in Data Security Principles, Cryptography, and Advanced Cryptography, and focuses on the analysis, evaluation, and breaking of cryptographic systems. The course examines classical and modern cryptanalytic techniques used to assess the security of symmetric and asymmetric cryptographic algorithms and protocols. Topics include statistical attacks, brute-force methods, frequency analysis, differential and linear cryptanalysis, side-channel attack awareness, protocol weaknesses, implementation vulnerabilities, and attacks against weak randomness and key management practices. Students also study the security assumptions, strengths, and limitations of modern cryptographic systems through practical analysis and comparative evaluation. The course includes laboratory activities and hands-on exercises that develop practical skills in cryptographic analysis, attack simulation, security evaluation, and vulnerability assessment within controlled and ethical environments.			

Module 34

Code	Course/Module Title	ECTS	Semester
------	---------------------	------	----------

CYS317	Cloud Computing	3	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
3	0	48	27
Description			
Cloud Computing builds upon the foundational knowledge acquired in computer networks and operating systems courses and introduces the principles, architectures, and technologies of modern cloud computing environments. The course covers cloud service models, virtualization, distributed systems, cloud infrastructure, storage systems, resource management, scalability, and cloud deployment models. Students study the design and operation of cloud platforms, data centers, containerization concepts, and cloud-based application hosting and services. The course also introduces fundamental concepts related to cloud security, availability, reliability, and data protection in virtualized and distributed environments. Emphasis is placed on understanding the architecture, management, and operational challenges of modern cloud computing systems and services.			

Module 35

Code	Course/Module Title	ECTS	Semester
CYS378	Network Security	6	6
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Network Security builds upon the concepts introduced in computer networks, cybersecurity fundamentals, and cryptography courses, and focuses on securing modern communication networks and networked systems against cyber threats and unauthorized access. The course covers network security architectures, firewalls, intrusion detection and prevention systems, virtual private networks, wireless network security, network monitoring, traffic analysis, access control mechanisms, and secure network design principles. Students study common network attacks, vulnerabilities, and defensive techniques used to protect enterprise and distributed network environments. The course also examines secure communication protocols, network hardening, and security policy implementation. Practical laboratory activities and hands-on exercises are integrated throughout the course to develop skills in configuring, analyzing, monitoring, and defending secure network infrastructures using modern security tools and technologies.			

Module 36

Code	Course/Module Title	ECTS	Semester
CYS348	Penetration Testing II	6	6
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	3	78	72

Description
Penetration Testing II extends the concepts and practical skills introduced in Penetration Testing I and focuses on advanced penetration testing methodologies, exploitation techniques, and security assessment practices in complex computing environments. As a high-ECTS course, it emphasizes advanced network and web application testing, privilege escalation, post-exploitation techniques, wireless security assessment, evasion methods, and controlled exploitation of modern system vulnerabilities. Students also study attack chaining, lateral movement concepts, security assessment methodologies, and professional penetration testing reporting practices. The course includes extensive laboratory activities and intensive hands-on practical exercises conducted in isolated and authorized environments using modern security tools, virtual machines, and realistic attack scenarios. Emphasis is placed on technical proficiency, analytical thinking, ethical considerations, and the practical application of offensive security techniques to evaluate and improve organizational security defenses.

Module 37

Code	Course/Module Title	ECTS	Semester
CYS335	Coding and Information Theory	5	6
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Coding and Information Theory introduces the fundamental principles of information representation, transmission, compression, and error control in digital communication systems. The course covers core information theory concepts such as entropy, redundancy, source coding, and channel capacity, together with practical coding techniques used for reliable data storage and transmission. Topics include file structures and multimedia formats, file headers, data compression techniques, transform methods such as the Fast Fourier Transform (FFT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and error detection and correction methods including Hamming codes and Reed-Solomon error correction codes. The course also examines how coding and signal representation techniques are applied in multimedia processing, secure communication, and digital data protection. Practical laboratory activities and MATLAB-based experiments are integrated throughout the course to develop hands-on skills in coding, compression, signal analysis, image and audio processing, and data representation. The course provides the theoretical and practical foundation required for advanced study in digital watermarking, steganography, multimedia security, and information hiding techniques.			

Module 38

Code	Course/Module Title	ECTS	Semester
CYS316	Artificial Intelligence	4	6
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	37

Description
Artificial Intelligence introduces the fundamental concepts, techniques, and applications of intelligent systems and computational decision-making. The course covers core topics such as intelligent agents, search algorithms, knowledge representation, reasoning systems, machine learning fundamentals, expert systems, and introductory neural network concepts. Students study how artificial intelligence techniques are used to solve complex computational problems, automate decision-making processes, and analyze data in modern computing environments. The course also introduces practical applications of artificial intelligence in areas such as cybersecurity, automation, pattern recognition, and data analysis. Emphasis is placed on understanding the theoretical foundations, algorithmic approaches, and real-world applications of intelligent systems.

Fourth year

Module 39

Code	Course/Module Title	ECTS	Semester
CYS498	Malware & Vulnerability Analysis	7	7
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	97
Description			
Malware and Vulnerability Analysis introduces the principles, techniques, and tools used to analyze malicious software and identify security vulnerabilities in modern computing systems. The course covers malware classification, behavior analysis, reverse engineering fundamentals, static and dynamic analysis techniques, vulnerability assessment, exploit concepts, and secure mitigation practices. Students study different types of malware such as viruses, worms, trojans, ransomware, spyware, and rootkits, together with the mechanisms used for persistence, obfuscation, and system compromise. The course also examines software and system vulnerabilities, vulnerability discovery methods, exploit development concepts, and security patching strategies. Strong emphasis is placed on laboratory work and hands-on practical analysis using isolated and controlled environments to develop technical skills in malware investigation, vulnerability analysis, threat understanding, and defensive security evaluation.			

Module 40

Code	Course/Module Title	ECTS	Semester
CYS478	Mobile & Network Security	6	7
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72

Description
Mobile and Network Security examines the security challenges, threats, and protection mechanisms associated with mobile devices, wireless communication, and modern networked environments. The course covers mobile operating system security, wireless network security, mobile application security, secure communication techniques, authentication methods, and access control mechanisms for mobile and distributed systems. Students study vulnerabilities and attacks targeting smartphones, wireless protocols, mobile applications, and network infrastructures, together with techniques used for monitoring, analysis, and defense. Topics also include secure mobile communication, device management, network hardening, and security considerations in modern wireless and mobile computing environments. Practical laboratory activities and hands-on exercises are integrated throughout the course to develop skills in analyzing, securing, and evaluating mobile and networked systems using modern cybersecurity tools and techniques.

Module 41

Code	Course/Module Title	ECTS	Semester
CYS486	Machine Learning for Cyber Security	5	7
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Machine Learning for Cybersecurity is an elective course that introduces the application of machine learning and artificial intelligence techniques in modern cybersecurity operations and defense strategies. The course covers the fundamental concepts of machine learning, data analysis, feature extraction, classification, anomaly detection, and predictive modeling within cybersecurity contexts. Students study the use of AI-driven techniques for malware detection, intrusion detection, threat intelligence, vulnerability analysis, behavioral monitoring, automated security assessment, and intelligent security monitoring systems. The course also explores the emerging role of autonomous and agent-based AI systems in cybersecurity, including AI-assisted penetration testing, security analysis agents, and the deployment of private and locally hosted security models for monitoring and controlled offensive security tasks. Ethical considerations, responsible AI usage, security risks, and the limitations of AI-driven cybersecurity systems are emphasized throughout the course. Practical laboratory activities and hands-on experiments are integrated to develop skills in building, training, deploying, and evaluating machine learning and AI-based solutions for real-world cybersecurity applications.			

Module 42

Code	Course/Module Title	ECTS	Semester
CYS419	Digital Forensics	5	7
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)

2	2	63	62
Description			
Digital Forensics introduces the principles, methodologies, and tools used in the identification, preservation, analysis, and presentation of digital evidence in cybersecurity investigations. The course covers forensic procedures for computer systems, storage devices, operating systems, networks, and mobile devices, with emphasis on maintaining evidence integrity and following proper investigative practices. Students study file systems, data recovery, log analysis, memory analysis, timeline reconstruction, network forensics, and malware-related investigations. The course also examines legal and ethical considerations related to digital evidence handling, chain of custody, and forensic reporting. Practical laboratory activities and hands-on investigations are integrated throughout the course to develop technical skills in forensic acquisition, analysis, incident investigation, and evidence documentation using modern forensic tools and controlled environments.			

Module 43

Code	Course/Module Title	ECTS	Semester
CYS439	Steganography & Watermarking	5	7
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Steganography and Watermarking introduces the fundamental principles, techniques, and applications of information hiding and digital media protection. The course covers methods for concealing and embedding information within digital media such as images, audio, video, and text, with emphasis on both steganographic and digital watermarking approaches. Students study spatial and transform-domain techniques, multimedia representation, perceptual transparency, robustness, fragile and semi-fragile watermarking, authentication methods, and information hiding security concepts. Topics also include detection and analysis of hidden information, basic steganalysis techniques, multimedia integrity protection, copyright protection, and tamper detection mechanisms. The course builds upon concepts introduced in Coding and Information Theory and related multimedia processing topics, including transforms such as FFT and DCT. Practical laboratory activities and hands-on experiments using multimedia processing and analysis tools are integrated throughout the course to develop skills in designing, implementing, analyzing, and evaluating secure information hiding and watermarking systems.			

Module 44

Code	Course/Module Title	ECTS	Semester
CYS404	Research Methodology	2	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USSWL (hr/w)
2	0	32	18

Description
Research Methodology introduces the fundamental principles, methods, and practices of scientific research in computing and cybersecurity disciplines. The course covers the research process, problem identification, literature review, research design, data collection methods, experimental and analytical approaches, and academic writing techniques. Students learn how to formulate research questions, evaluate scholarly sources, conduct ethical research, analyze results, and present findings in a clear and structured manner. The course also introduces citation standards, plagiarism awareness, research integrity, and the preparation of technical reports, proposals, and scientific papers. Emphasis is placed on developing critical thinking, analytical skills, and the ability to conduct independent research in academic and professional environments.

Module 45

Code	Course/Module Title	ECTS	Semester
CYS487	Internet of Things Security	5	8
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Internet of Things Security examines the security challenges, threats, and protection mechanisms associated with interconnected smart devices and embedded systems in modern Internet of Things (IoT) environments. The course covers IoT architectures, communication protocols, embedded device security, wireless communication security, authentication methods, access control, firmware security, and secure data transmission in resource-constrained systems. Students study common IoT vulnerabilities, attack vectors, botnets, device exploitation techniques, and methods for securing smart devices, sensors, and industrial IoT infrastructures. The course also explores privacy concerns, cloud-connected IoT systems, secure update mechanisms, and risk management in large-scale IoT deployments. Practical laboratory activities and hands-on exercises are integrated throughout the course to develop skills in analyzing, configuring, monitoring, and securing IoT devices and communication environments using modern cybersecurity tools and techniques.			

Module 46

Code	Course/Module Title	ECTS	Semester
CYS449	Blockchain Technology	4	8
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	37
Description			
Blockchain Technology introduces the fundamental concepts, architectures, and applications of blockchain and distributed ledger systems. The course covers decentralized networks, block structures, cryptographic hashing, consensus mechanisms, digital			

signatures, smart contracts, and transaction validation processes. Students study the operational principles of blockchain platforms, distributed trust models, and the role of cryptography in maintaining integrity, transparency, and immutability within decentralized systems. The course also examines blockchain security challenges, privacy considerations, cryptocurrency fundamentals, and real-world applications in finance, cybersecurity, digital identity, and secure data management. Emphasis is placed on understanding the technical foundations, security implications, and emerging applications of blockchain technologies in modern computing environments.

Module 47

Code	Course/Module Title	ECTS	Semester
CYS441	Mobile Applications Development	5	8
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	2	63	62
Description			
Mobile Applications Development introduces the fundamental concepts, tools, and techniques used in the design and development of modern mobile applications. The course covers mobile application architecture, user interface design, event-driven programming, local data storage, network communication, API integration, and mobile application deployment. Students learn how to develop interactive and responsive applications for mobile platforms using modern development frameworks and programming tools. The course also introduces secure mobile development practices, including permission management, secure data handling, authentication mechanisms, and protection against common mobile application vulnerabilities. Practical laboratory activities and hands-on projects are integrated throughout the course to develop technical skills in designing, implementing, testing, and deploying mobile applications in modern mobile computing environments.			

Module 48

Code	Course/Module Title	ECTS	Semester
CYS459	Authentication and Access Control	6	8
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Authentication and Access Control introduces the fundamental principles, models, and technologies used to verify identities and regulate access to digital systems and resources. The course covers authentication mechanisms, password security, multi-factor authentication, biometrics, authorization models, role-based and attribute-based access control, identity management, and session security. Students study access control policies, privilege management, federated identity systems, single sign-on technologies, and secure			

authentication protocols used in modern computing environments. The course also examines common authentication attacks, credential theft, privilege escalation, and methods for strengthening identity and access management systems. Practical laboratory activities and hands-on exercises are integrated throughout the course to develop skills in implementing, configuring, analyzing, and securing authentication and access control mechanisms in modern information systems.

Module 49

Code	Course/Module Title	ECTS	Semester
CYS418	Operating Systems Security	6	8
Class (hr/w)	Lab (hr/w)	SSWL (hr/sem)	USSWL (hr/w)
3	2	78	72
Description			
Operating Systems Security builds upon the concepts introduced in Operating Systems and focuses on securing modern desktop, server, and enterprise operating environments against cyber threats and unauthorized access. The course covers operating system hardening, access control mechanisms, privilege management, process and memory protection, secure authentication, auditing, logging, virtualization security, and malware defense techniques. Students study security features and vulnerabilities in both Microsoft Windows and Linux operating systems, including user and group management, permissions, firewall configuration, system monitoring, and secure server administration. The course also examines attack techniques targeting operating systems, escalation methods, persistence mechanisms, and defensive security practices used to protect host systems. Strong emphasis is placed on practical laboratory work and hands-on system administration and security exercises conducted in desktop and server environments to develop real-world operating system security skills.			

Module 50

Code	Course/Module Title	ECTS	Semester
CYS414	Graduation Project	4	8
Practical (Hr/w)	Seminar (Hr/w)	SSWL (hr/sem)	USSWL (hr/w)
2	1	47	53
Description			
Graduation Project is a capstone course that provides students with the opportunity to apply the knowledge and skills acquired throughout the cybersecurity program to a substantial practical, research, or development project. Students work individually or in teams under academic supervision to identify a problem, conduct research, design and implement a solution, and evaluate its effectiveness using appropriate methodologies and tools. Projects may involve areas such as cybersecurity, network security, software development, digital forensics, cryptography, artificial intelligence, or other related fields. The course emphasizes project planning, problem-solving, technical documentation,			

professional presentation, and ethical considerations, culminating in a final report and project defense.

3. Contact

Program Manager:

Asst. Prof. Dr. Ahmad A. AlSabhany | Ph.D. in Computer Science – Data Security | Assistant Professor

Email: ahmad.alsabhany@uofallujah.edu.iq

Mobile no.: 7807167888