

University of Mosul

جامعة الموصل



College of Computer Science and Mathematics – Department of Cyber Security

كلية علوم الحاسوب والرياضيات – قسم الأمن السيبراني

Bachelor's Degree (B.Sc.) in Cyber Security

Table of Contents

1. Overview
 2. Undergraduate Modules 2026-2027
 3. Contact
-

1. Overview

This catalogue is about the courses (modules) given by the program of Cyber Security to gain the Bachelor of Science degree. The program delivers (51) Modules with (6000) total student workload hours and 240 total ECTS. The module delivery is based on the Bologna Process.

نظرة عامة

يتناول هذا الدليل المواد الدراسية التي يقدمها برنامج قسم الأمن السيبراني للحصول على درجة بكالوريوس العلوم. يقدم البرنامج (51) مادة دراسية، بإجمالي (6000) ساعة حمل دراسي للطلاب و(240) وحدة أوروبية. يعتمد تقديم المواد الدراسية على عملية بولونيا.

2. Undergraduate Modules 2026-2027

Module 1

Code	Course/Module Title	ECTS	Semester
CYBS-101	Programming (1)	8	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	122
Description			
This module introduces the fundamentals of computer programming and algorithmic problem solving using Python. Students learn how to analyse a problem, design an algorithm with flowcharts and pseudocode, and translate it into working code. Topics include the programming environment, variables and data types, operators and expressions, input and output, conditional statements, loops, and nested control structures. The module then covers functions and parameter passing, strings and string manipulation, lists, tuples, and basic debugging and testing techniques. Laboratory sessions give students hands-on practice in writing, running, and correcting programs, and in developing small programs that solve practical problems. The module builds the programming foundation required for all later programming and security-tool development modules in the program.			

Module 2

Code	Course/Module Title	ECTS	Semester
CYBS-102	Discrete Structures (1)	4	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module provides the mathematical foundations of computer science and cyber security. It covers propositional logic, truth tables, logical equivalence, predicates and quantifiers, and rules of inference. Students study methods of proof, including direct proof, proof by contradiction, and mathematical induction. The module then introduces set theory and set operations, relations and their properties, equivalence relations and partial orders, and functions, including injective, surjective, and bijective functions and their composition and inverses. Basic counting principles, permutations, combinations, and the pigeonhole principle are also covered. Tutorial sessions focus on solving problems and developing rigorous logical reasoning, which supports later study of algorithms, cryptography, and formal security models.			

Module 3

Code	Course/Module Title	ECTS	Semester
CYBS-103	Logic Design Fundamentals	6	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	87
Description			
This module introduces the principles of digital logic design that underlie all computing hardware. Topics include number systems and conversions, binary arithmetic, complements, and binary codes. Students study Boolean algebra, basic and universal logic gates, canonical forms, and the simplification of Boolean functions using algebraic methods and Karnaugh maps. The module then covers the analysis and design of combinational circuits such as adders, subtractors, comparators, encoders, decoders, multiplexers, and demultiplexers, and introduces latches and flip-flops as the basis of sequential circuits. Laboratory sessions allow students to build, simulate, and test logic circuits, strengthening their understanding of how data is represented and processed at the hardware level.			

Module 4

Code	Course/Module Title	ECTS	Semester
CYBS-104	Information Security Principles	5	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module introduces the core concepts of information security. Students study the security goals of confidentiality, integrity, and availability, together with authentication, authorisation, accountability, and non-repudiation. The module explains threats, vulnerabilities, risks, and the main categories of attacks, and introduces security policies, standards, and procedures. Topics include identification and authentication methods, passwords and multi-factor authentication, access control models, basic cryptographic concepts, physical security, and security awareness. Students are also introduced to the legal and ethical dimensions of information security. Laboratory sessions provide practical exposure to basic security configurations and tools, preparing students for the specialised security modules that follow in the program.			

Module 5

Code	Course/Module Title	ECTS	Semester
CYBS-105	Calculus	3	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	27
Description			
This module develops the calculus skills required in computing and engineering applications. It begins with functions, their domains, ranges, graphs, and inverses, and then covers limits, limits involving infinity, and continuity. Students study the derivative, its definition and rules of differentiation, the chain rule, implicit differentiation, and derivatives of trigonometric, exponential, logarithmic, and inverse functions. Applications of derivatives include rates of change, extreme values, the mean value theorem, curve sketching, and optimisation problems. The module concludes with an introduction to integration, the fundamental theorem of calculus, and basic techniques and applications of integrals. Tutorial sessions focus on problem solving and on building mathematical fluency.			

Module 6

Code	Course/Module Title	ECTS	Semester
UOM1021	English Language (1)	2	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module develops students' general English language proficiency by integrating the four skills of reading, writing, speaking, and listening. The module reviews and consolidates core grammar, including verb tenses, question forms, articles, and sentence structure, and expands everyday and academic vocabulary. Students practise reading short texts for main ideas and detail, writing simple and well-structured paragraphs, and communicating in common social and academic situations. Emphasis is placed on motivating activities and on autonomous learning, so that students acquire strategies to continue improving their English through self-study. The module prepares students to read technical material in English, which is essential in the field of cyber security.			

Module 7

Code	Course/Module Title	ECTS	Semester
UOM1040	Democracy and Human Rights	2	1
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module introduces students to the concepts of democracy and human rights and their importance in modern societies. It covers the historical development of human rights, their sources in religion, philosophy, and international law, and the main international declarations and covenants. Students study civil and political rights, economic, social, and cultural rights, and the rights of specific groups, together with the guarantees that protect these rights at the national and international levels. The module also explains the principles of democracy, elections, the separation of powers, and the role of civil society, with reference to the Iraqi Constitution. It aims to build responsible citizenship, respect for others, and awareness of rights and duties.			

Module 8

Code	Course/Module Title	ECTS	Semester
CYBS-107	Advanced Programming	7	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	97
Description			
This module builds on Programming (1) and develops students' ability to write larger, well-structured, and reusable Python programs. Topics include advanced functions, recursion, lambda expressions, modules and packages, and the use of standard libraries. Students work with dictionaries and sets, file handling, exception handling, and regular expressions for text and log processing. The module introduces scripting for automation, working with the operating system and command-line arguments, and basic network and socket programming. Throughout the module, examples are drawn from security-related tasks such as parsing logs, processing data files, and building simple utilities. Laboratory sessions emphasise program design, testing, and debugging, and prepare students to develop their own security tools.			

Module 9

Code	Course/Module Title	ECTS	Semester
CYBS-108	Computer Organization	6	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	72
Description			
This module explains how a computer system is organised and how its components work together. Students study the basic structure of the computer, the von Neumann model, and data representation. The module covers the central processing unit, registers, the arithmetic and logic unit, the control unit, and the instruction cycle. Topics include instruction formats, addressing modes, and an introduction to assembly language programming. Students also study the memory hierarchy, main memory, cache concepts, and secondary storage, as well as buses, input and output organisation, interrupts, and direct memory access. Laboratory sessions use simulators and assembly exercises, giving students the low-level understanding required for later study of operating systems, malware analysis, and software security.			

Module 10

Code	Course/Module Title	ECTS	Semester
CYBS-109	Cyber Security Fundamentals	5	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module provides a broad introduction to the field of cyber security. Students study the cyber threat landscape, threat actors and their motivations, and the main categories of attacks, including malware, phishing and social engineering, password attacks, denial of service, and web and network attacks. The module introduces defensive concepts such as defence in depth, security controls, firewalls, antivirus and intrusion detection, secure configuration, backups, and patch management. Students are introduced to security operations, incident response, and the basics of digital evidence, as well as cyber laws, ethics, and professional conduct. Laboratory sessions provide hands-on exposure to common attacks and defences in a controlled environment, forming the basis for the specialised modules later in the program.			

Module 11

Code	Course/Module Title	ECTS	Semester
CYBS-110	Discrete Structures (2)	4	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module continues Discrete Structures (1) and focuses on structures that are central to algorithms and cryptography. Topics include advanced counting techniques, the inclusion-exclusion principle, and recurrence relations and their solution. Students study elementary number theory, including divisibility, prime numbers, the greatest common divisor, the Euclidean algorithm, modular arithmetic, and congruences. The module then introduces graph theory, including graph representations, paths and circuits, connectivity, Euler and Hamilton paths, shortest paths, and graph colouring, followed by trees, spanning trees, and tree traversal. Boolean algebra and an introduction to algebraic structures are also covered. Tutorial sessions strengthen problem-solving skills needed in data structures, networks, and cryptography.			

Module 12

Code	Course/Module Title	ECTS	Semester
CYBS-111	Probabilities & Statistics	3	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	27
Description			
This module introduces the probability and statistics concepts used in data analysis, networking, and security. Students study descriptive statistics, including data types, frequency distributions, graphical representation, measures of central tendency, and measures of dispersion. The module then covers the basic concepts of probability, sample spaces and events, counting methods, conditional probability, independence, and Bayes' theorem. Students study discrete and continuous random variables, expectation and variance, and important distributions such as the binomial, Poisson, uniform, exponential, and normal distributions. An introduction to correlation and simple linear regression completes the module. Tutorial sessions apply these tools to practical problems, including examples from anomaly detection and risk estimation.			

Module 13

Code	Course/Module Title	ECTS	Semester
UOM1011	Arabic Language (1)	2	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module aims to strengthen students' command of the Arabic language in reading, writing, and expression. It covers essential rules of Arabic grammar and morphology that are most needed in everyday and academic writing, together with correct spelling, including the rules of writing the hamza and common spelling errors. Students study punctuation marks and their correct use, and the basics of sentence and paragraph construction. The module also includes selected texts from the Holy Quran, poetry, and prose, which are read and analysed to develop linguistic taste and comprehension. The module prepares students to write clear, correct Arabic in official letters, reports, and academic work.			

Module 14

Code	Course/Module Title	ECTS	Semester
UOM1031	Computer	3	2
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / 1 / - / -	48	27
Description			
This university-requirement module develops the essential computer skills that students need throughout their studies. It introduces the components of a computer, hardware and software, and the use of the operating system for managing files and folders. Students learn word processing, including creating, formatting, and printing documents, inserting tables, images, and equations, and preparing reports. The module also covers spreadsheets, including data entry, formulas, functions, and charts, and presentation software for designing effective slides. Basic use of the Internet, e-mail, and online services is included, together with principles of safe computer use, protection from malware, and password hygiene. Laboratory sessions provide practical training in all topics.			

Module 15

Code	Course/Module Title	ECTS	Semester
CYBS-201	Object-Oriented Programming (1)	8	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	122
Description			
This module introduces the object-oriented programming paradigm and its role in building maintainable and secure software. Students learn the difference between procedural and object-oriented design, and study classes and objects, attributes and methods, constructors and destructors, and access modifiers. The module covers encapsulation and data hiding, object composition, static members, method overloading, and the basics of inheritance. Students also work with arrays and collections of objects, strings, and simple class diagrams to model problems before implementing them. Laboratory sessions focus on designing and implementing small object-oriented applications, applying good coding style, and testing and debugging programs, laying the foundation for Object-Oriented Programming (2).			

Module 16

Code	Course/Module Title	ECTS	Semester
CYBS-202	Data Structures	5	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module introduces the fundamental data structures and algorithms used to organise and process data efficiently. Students study algorithm analysis and Big-O notation, then arrays, records, and matrices. The module covers linear structures, including stacks, queues, circular and priority queues, and singly, doubly, and circular linked lists, with their applications such as expression evaluation. Students then study recursion, trees, binary trees, binary search trees, tree traversal, heaps, and an introduction to graphs and graph traversal. Hashing and hash tables are also covered, together with classic searching and sorting algorithms and their comparison. Laboratory sessions require students to implement these structures, which supports later work in databases, networks, and security tools.			

Module 17

Code	Course/Module Title	ECTS	Semester
CYBS-203	Computational Theory	3	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	27
Description			
This module introduces the theoretical foundations of computation. Students study formal languages, alphabets, and strings, and then finite automata, both deterministic and non-deterministic, and their equivalence. The module covers regular expressions, regular languages, and their properties, including the pumping lemma. Students then study context-free grammars, derivations and parse trees, ambiguity, simplification of grammars, and pushdown automata. The module concludes with Turing machines, the Church-Turing thesis, and an introduction to decidability and computability. Tutorial sessions focus on designing automata and grammars and on solving problems. These concepts support later study of compilers, input validation, and pattern matching used in intrusion detection.			

Module 18

Code	Course/Module Title	ECTS	Semester
CYBS-204	Database Basics	4	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	37
Description			
This module introduces the principles of database systems and relational database design. Students study the limitations of file-based systems, database architecture, data models, and the roles of the database management system. The module covers conceptual design using the entity-relationship model, the relational model, keys, and integrity constraints, and the mapping of ER diagrams to relational schemas. Students learn relational algebra and the Structured Query Language (SQL), including data definition, data manipulation, joins, subqueries, grouping, and views. Functional dependencies and normalisation up to Boyce-Codd normal form are also covered. Laboratory sessions give practical experience in creating and querying databases, preparing students for Distributed Databases and Database Security.			

Module 19

Code	Course/Module Title	ECTS	Semester
CYBS-205	Cryptography (1)	8	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	122
Description			
This module introduces the principles and techniques of cryptography, the core technology for protecting data. It begins with basic terminology, the history of cryptography, and cryptanalysis concepts. Students study classical ciphers, including substitution, transposition, Caesar, monoalphabetic, Playfair, Hill, and Vigenere ciphers, and methods for breaking them. The module covers the mathematical background of modular arithmetic, then modern symmetric-key cryptography, including stream ciphers, block ciphers, Feistel structures, the Data Encryption Standard, and the Advanced Encryption Standard, together with block cipher modes of operation. Laboratory sessions require students to implement ciphers and attacks in code, strengthening their practical and analytical understanding of encryption.			

Module 20

Code	Course/Module Title	ECTS	Semester
UOM2022	English Language (2)	2	3
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module continues English Language (1) for students who already have a basic foundation in the language. New grammar is introduced systematically, including perfect tenses, modal verbs, conditionals, the passive voice, and reported speech, followed by controlled and freer practice activities. Vocabulary is expanded regularly, with attention to technical and academic words used in computing. Students practise reading longer texts, writing structured paragraphs and short reports, and taking part in conversations and discussions to build fluency and confidence. The module aims to raise overall English proficiency so that students can read technical documentation, understand security literature, and communicate effectively in English.			

Module 21

Code	Course/Module Title	ECTS	Semester
CYBS-207	Object-Oriented Programming (2)	7	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
5	2 / 2 / - / 1	78	97
Description			
This module continues Object-Oriented Programming (1) and develops advanced object-oriented design and programming skills. Students study inheritance hierarchies, method overriding, polymorphism, abstract classes, and interfaces. The module covers exception handling, generic programming, collections and data structures in the standard library, and file and stream input and output, including object serialisation. Students are introduced to graphical user interface programming, event handling, and multithreading. The module also introduces secure coding practices in object-oriented programs, such as input validation and safe error handling. Laboratory sessions and a mini project require students to design and implement a complete application using sound object-oriented principles.			

Module 22

Code	Course/Module Title	ECTS	Semester
CYBS-208	Cyber Security Tools	5	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	48	77
Description			
This module provides practical training in the tools used by cyber security professionals. Students work in a Linux-based security environment and learn command-line administration and scripting. The module covers information gathering and network scanning tools, packet capture and traffic analysis tools, vulnerability scanners, password-auditing tools, and web proxy tools for testing web applications. Students are introduced to exploitation frameworks, firewall and intrusion detection configuration, and log analysis tools. Each tool is studied in terms of its purpose, operation, output interpretation, and limitations. All exercises are carried out in an isolated laboratory under an ethical and legal framework, preparing students for Ethical Hacking, Network Security, and Digital Forensics.			

Module 23

Code	Course/Module Title	ECTS	Semester
CYBS-209	Distributed Databases	4	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	37
Description			
This module extends Database Basics to database systems whose data is stored across multiple sites. Students study distributed database architectures, the benefits and challenges of distribution, and distributed database design, including horizontal, vertical, and mixed fragmentation, replication, and allocation. The module covers distributed query processing and optimisation, distributed transaction management, concurrency control, deadlock handling, and recovery, including the two-phase commit protocol. Students are also introduced to data reliability, client- server and cloud database models, and NoSQL databases. Laboratory sessions provide practical experience in building and querying distributed and replicated databases, and highlight the security and availability issues that arise in distributed data environments.			

Module 24

Code	Course/Module Title	ECTS	Semester
CYBS-210	Software Security	5	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	77
Description			
This module studies how security flaws are introduced into software and how to prevent them. Students learn the principles of secure software design and the secure software development life cycle. The module covers common vulnerability classes, including buffer overflows, integer overflows, format string flaws, race conditions, injection flaws, and improper input validation and error handling. Students study memory safety, secure use of libraries, authentication and session handling in code, and secure storage of sensitive data. Techniques for finding vulnerabilities, such as code review, static analysis, dynamic analysis, and fuzzing, are introduced, together with defensive coding practices and mitigation mechanisms. Tutorial sessions analyse real vulnerable code examples.			

Module 25

Code	Course/Module Title	ECTS	Semester
CYBS-211	Cryptography (2)	5	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	48	77
Description			
This module continues Cryptography (1) and focuses on public-key cryptography and data integrity. Students study the number theory behind public-key systems, including prime numbers, primality testing, Euler's and Fermat's theorems, the Chinese remainder theorem, and discrete logarithms. The module covers the RSA cryptosystem, Diffie-Hellman key exchange, ElGamal encryption, and an introduction to elliptic curve cryptography. Students then study cryptographic hash functions, message authentication codes, digital signatures, key management and distribution, and public key infrastructure and digital certificates. Laboratory sessions require students to implement and test these algorithms and to analyse common attacks against them.			

Module 26

Code	Course/Module Title	ECTS	Semester
UOM2050	Ba'ath Crimes in Iraq	2	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module, mandated by the Ministry of Higher Education and Scientific Research, studies the crimes and violations committed in Iraq during the period of the former Ba'ath regime. It covers the concept of crime and its types under national and international law, and the political, security, and social circumstances of that period. Students study documented cases such as political repression and executions, forced displacement, the Anfal campaigns, the chemical attack on Halabja, the mass graves, and the destruction of the environment, including the draining of the marshes. The module also introduces the legal and institutional mechanisms of transitional justice in Iraq and the importance of documenting and preserving historical memory.			

Module 27

Code	Course/Module Title	ECTS	Semester
UOM2012	Arabic Language (2)	2	4
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
2	2 / - / - / -	32	18
Description			
This university-requirement module continues Arabic Language (1) and further develops students' linguistic and writing skills. It covers additional rules of grammar and morphology, common linguistic errors and their corrections, and the correct use of numbers and their agreement. Students practise the skills of administrative and academic writing, including official letters, reports, summaries, and research writing, with attention to clarity, organisation, and accuracy. Selected literary texts are read and analysed to strengthen comprehension and expression. The module aims to enable students to write sound Arabic in their professional and academic work, including the documentation of technical and research projects.			

Module 28

Code	Course/Module Title	ECTS	Semester
CYBS-301	Coding and Information Theory	6	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	102
Description			
This module introduces the mathematical theory of information and coding and its relevance to communication and security. Students study the measurement of information, entropy, joint and conditional entropy, and mutual information. The module covers source coding, including prefix codes, the Kraft inequality, Shannon-Fano coding, Huffman coding, arithmetic coding, and dictionary-based compression. Students then study communication channels, channel capacity, and Shannon's theorems, followed by error detection and correction, including parity, Hamming codes, linear block codes, cyclic codes, and cyclic redundancy checks. The module also discusses Shannon's theory of secrecy and perfect secrecy, linking information theory to cryptography.			

Module 29

Code	Course/Module Title	ECTS	Semester
CYBS-302	Cloud Computing Principles	5	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module introduces the concepts, technologies, and service models of cloud computing. Students study the characteristics of cloud computing, the service models of Infrastructure, Platform, and Software as a Service, and public, private, community, and hybrid deployment models. The module covers virtualisation, hypervisors, virtual machines, and containers, as well as cloud storage, networking, elasticity, scalability, and load balancing. Students are introduced to service-level agreements, cloud economics, and an overview of cloud security challenges. Laboratory sessions provide hands-on experience in creating and managing virtual machines and containers and in deploying simple services on a cloud platform, preparing students for Cloud Computing Security.			

Module 30

Code	Course/Module Title	ECTS	Semester
CYBS-303	Computer Networks	5	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module provides a comprehensive introduction to computer networks. Students study network types, topologies, and the OSI and TCP/IP reference models. The module covers the physical and data link layers, including transmission media, framing, error control, Ethernet, switching, and VLANs. Students then study the network layer, including IPv4 and IPv6 addressing, subnetting, and routing concepts and protocols, and the transport layer, including TCP, UDP, flow control, and congestion control. Application-layer protocols such as DNS, DHCP, HTTP, and e-mail protocols are also covered. Laboratory sessions use network simulators and packet analysers to configure networks and inspect traffic, forming the basis for Network Security and Secure Communication Protocols.			

Module 31

Code	Course/Module Title	ECTS	Semester
CYBS-304	Malicious Codes Analysis	6	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	87
Description			
This module teaches students how to analyse malicious software in order to understand its behaviour and defend against it. Students study malware types, including viruses, worms, Trojans, ransomware, rootkits, and botnets, and their infection and persistence mechanisms. The module covers the set-up of a safe analysis environment, basic static analysis of file formats, strings, and imports, and dynamic analysis using sandboxes and monitoring tools. Students are introduced to disassembly and reverse engineering, packing and obfuscation techniques, and anti-analysis tricks. The extraction of indicators of compromise and the writing of detection signatures are also covered. All laboratory work is performed in isolated environments following strict ethical rules.			

Module 32

Code	Course/Module Title	ECTS	Semester
CYBS-305	Artificial Intelligence	4	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	37
Description			
This module introduces the principles and techniques of artificial intelligence. Students study intelligent agents and problem formulation, uninformed search methods, heuristic search such as A*, and adversarial search in games. The module covers knowledge representation and reasoning using propositional and first-order logic, rule-based systems, and reasoning under uncertainty. Students are introduced to machine learning, including supervised and unsupervised learning, decision trees, and basic neural networks, together with the evaluation of learning models. Applications of artificial intelligence in cyber security, such as spam filtering and intrusion detection, are discussed. Laboratory sessions implement search and learning algorithms in Python, preparing students for Intelligent Analysis of Security Threats.			

Module 33

Code	Course/Module Title	ECTS	Semester
CYBS-306	Computer Architecture	4	5
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module builds on Computer Organization and examines the design principles that determine computer performance. Students study performance measurement, instruction set architecture design, and the differences between RISC and CISC processors. The module covers datapath and control design, instruction pipelining, pipeline hazards and their resolution, and branch prediction. Students study the memory hierarchy in depth, including cache organisation, mapping and replacement policies, and virtual memory, as well as input and output systems. An introduction to parallel processing, multicore processors, and GPUs completes the module. Hardware-level security issues, such as side-channel attacks on caches, are highlighted to connect architecture with security.			

Module 34

Code	Course/Module Title	ECTS	Semester
CYBS-307	Compiler Design	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module explains how high-level programs are translated into executable code. Students study the structure and phases of a compiler, then lexical analysis using regular expressions and finite automata. The module covers syntax analysis with context-free grammars, top-down parsing including recursive descent and LL(1) parsing, and bottom-up parsing including LR parsing. Students then study syntax-directed translation, semantic analysis, symbol tables, type checking, intermediate code generation, code optimisation, and target code generation. The relationship between compilers and security, including input parsing flaws, code obfuscation, and compiler-based protections, is discussed. Laboratory sessions require students to build components of a simple compiler.			

Module 35

Code	Course/Module Title	ECTS	Semester
CYBS-308	Network Security	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module studies the threats facing computer networks and the technologies used to protect them. Students study network attacks, including reconnaissance, sniffing, spoofing, man-in-the-middle, session hijacking, and denial-of-service attacks. The module covers defensive technologies, including packet-filtering and stateful firewalls, proxies, network address translation, intrusion detection and prevention systems, virtual private networks, and network access control. Students also study secure network architecture and segmentation, wireless network security, and network monitoring and logging. Laboratory sessions require students to carry out attacks in an isolated environment and to configure firewalls, intrusion detection systems, and VPNs to defend against them.			

Module 36

Code	Course/Module Title	ECTS	Semester
CYBS-309	Database Security	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	77
Description			
This module focuses on protecting the confidentiality, integrity, and availability of data stored in database systems. Students study database security requirements and threats, user management, authentication, privileges, roles, and views as security mechanisms. The module covers discretionary, mandatory, and role-based access control in databases, SQL injection attacks and their prevention, the inference problem, and statistical database security. Students also study database auditing, encryption of data at rest and in transit, backup and recovery, and the security features of commercial database management systems. Privacy protection and data anonymisation are introduced. Tutorial sessions analyse security scenarios and design secure database configurations.			

Module 37

Code	Course/Module Title	ECTS	Semester
CYBS-310	Awareness and Training for Security	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	77
Description			
This module addresses the human dimension of cyber security. Students study why people are often the weakest link in security, and the techniques of social engineering, including phishing, pretexting, baiting, and impersonation. The module covers the design of security awareness and training programmes, including needs analysis, identifying target audiences, choosing delivery methods, developing content, and measuring effectiveness. Students study how to communicate security policies, promote a security culture within organisations, and run simulated phishing and awareness campaigns ethically. Tutorial sessions include case studies, discussions, and group work in which students prepare and present awareness material for a real institutional audience.			

Module 38

Code	Course/Module Title	ECTS	Semester
CYBS-311	Secure Communication Protocols	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	77
Description			
This module studies the protocols that provide secure communication over networks. Students review the security services and cryptographic building blocks used in protocols, then study authentication protocols and Kerberos. The module covers Transport Layer Security and HTTPS, IP Security and its modes and protocols, Secure Shell, and secure e-mail using PGP and S/MIME. Students also study DNS security extensions, wireless security protocols including WPA2 and WPA3, and secure protocols for remote access. Known attacks against protocols and the principles of protocol design and analysis are discussed. Tutorial sessions involve analysing protocol exchanges and captured traffic to understand how each protocol achieves its security goals.			

Module 39

Code	Course/Module Title	ECTS	Semester
CYBS-312	Ethical Hacking	5	6
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module teaches the methods used by attackers so that students can test and strengthen the security of systems in a lawful and authorised manner. Students study the legal and ethical framework of penetration testing, rules of engagement, and testing methodologies. The module covers the phases of a penetration test: reconnaissance and footprinting, scanning and enumeration, vulnerability analysis, exploitation, privilege escalation, maintaining access, and covering tracks, together with password attacks and attacks on web applications and wireless networks. Students learn to document findings and write professional penetration test reports with remediation recommendations. All laboratory work is carried out in isolated, purpose-built environments.			

Module 40

Code	Course/Module Title	ECTS	Semester
CYBS-401	Operating Systems	5	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module introduces the concepts and design of modern operating systems. Students study operating system structures and services, processes and threads, and CPU scheduling algorithms. The module covers process synchronisation, critical sections, semaphores, and monitors, together with deadlock characterisation, prevention, avoidance, and detection. Students then study memory management, paging, segmentation, and virtual memory, followed by file systems, storage management, and input and output systems. Protection mechanisms are introduced as a bridge to Operating Systems Security. Laboratory sessions use the Linux operating system to practise system administration, shell commands, and programming with processes and threads.			

Module 41

Code	Course/Module Title	ECTS	Semester
CYBS-402	Internet of Things (IoT) Security	4	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module studies the security of Internet of Things systems. Students study IoT architectures, devices, sensors, and gateways, and communication technologies and protocols such as MQTT, CoAP, Zigbee, and Bluetooth Low Energy. The module analyses the IoT attack surface, including device, firmware, network, and cloud vulnerabilities, and common attacks such as botnets and device hijacking. Students study security mechanisms suited to constrained devices, including lightweight cryptography, device authentication, secure boot, and secure firmware updates, together with IoT security frameworks and standards. The security of industrial control systems is also introduced. Tutorial sessions analyse real IoT incidents and propose secure designs.			

Module 42

Code	Course/Module Title	ECTS	Semester
CYBS-403	Web Applications Programming	5	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module teaches students how to design and build dynamic web applications. Students study the architecture of the web, the HTTP protocol, and client-server interaction. The module covers client-side development with HTML, CSS, and JavaScript, including forms, the document object model, and asynchronous requests. Students then study server-side programming, handling requests and responses, sessions and cookies, and connecting web applications to databases. The module introduces web frameworks, RESTful services, and data exchange formats such as JSON. Basic security considerations, such as input validation and authentication, are emphasised throughout. Laboratory sessions lead students to build a complete web application, preparing them for Web Applications Security.			

Module 43

Code	Course/Module Title	ECTS	Semester
CYBS-404	Electronic Governance Security	4	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module examines the security of electronic government services. Students study the concepts, models, and stages of e-government and e-governance, and the services provided to citizens, businesses, and government bodies. The module covers the security requirements of e-government systems, including identity management, electronic authentication, digital signatures, and public key infrastructure. Students study the protection of government data, privacy, trust, and availability of services, as well as the legal and regulatory frameworks that govern electronic transactions, with reference to Iraqi legislation. Threats facing e-government and national critical infrastructure, and strategies to counter them, are discussed through case studies.			

Module 44

Code	Course/Module Title	ECTS	Semester
CYBS-405	Cloud Computing Security	5	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module builds on Cloud Computing Principles and focuses on securing cloud environments. Students study the shared responsibility model, cloud threats and vulnerabilities, and the security architecture of cloud platforms. The module covers identity and access management, data protection and encryption in the cloud, key management, virtualisation and hypervisor security, container security, and secure network configuration in virtual networks. Students also study logging and monitoring, incident response in the cloud, governance, compliance, and cloud security standards and frameworks. Laboratory sessions require students to configure access policies, encrypt data, and harden and monitor cloud resources on a cloud platform.			

Module 45

Code	Course/Module Title	ECTS	Semester
CYBS-406	Project I	7	7
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	- / - / 3 / -	47	128
Description			
This module is the first part of the graduation research project. Under the supervision of a faculty member, students, individually or in small teams, select a research problem in cyber security. Students conduct a systematic literature review, define the problem, objectives, and scope, and identify the tools, datasets, and methods to be used. They prepare a project proposal and a detailed design of the proposed solution, and begin preliminary implementation or experimentation. Students present their work in seminars and submit a written report at the end of the semester. The module develops research, planning, technical writing, and presentation skills, and prepares students to complete the project in Project II.			

Module 46

Code	Course/Module Title	ECTS	Semester
CYBS-407	Operating Systems Security	5	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module studies how operating systems are attacked and how they are protected. Students study operating system security principles, trusted computing base, and security models. The module covers user authentication, access control models including discretionary, mandatory, and role-based access control, privilege management, and file system permissions in Linux and Windows. Students study operating system attacks such as privilege escalation, rootkits, and memory corruption, together with mitigation mechanisms such as address space layout randomisation, sandboxing, and security modules. System hardening, patch management, logging, and auditing are also covered. Laboratory sessions require students to harden, audit, and monitor Linux and Windows systems.			

Module 47

Code	Course/Module Title	ECTS	Semester
CYBS-408	Web Applications Security	5	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module studies the vulnerabilities of web applications and the methods used to secure them. Students study the web application attack surface and the most critical web security risks as identified by OWASP. The module covers injection attacks, cross-site scripting, cross-site request forgery, broken authentication and session management, access control flaws, insecure deserialisation, server-side request forgery, and security misconfiguration. Students learn secure development practices, security headers, and the testing of web applications using manual techniques and automated scanners. Laboratory sessions require students to discover and exploit vulnerabilities in intentionally vulnerable applications and then fix them in code.			

Module 48

Code	Course/Module Title	ECTS	Semester
CYBS-409	Digital Forensics	5	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
4	2 / 2 / - / -	63	62
Description			
This module introduces the scientific methods used to investigate digital incidents and crimes. Students study the digital forensic process, the legal requirements for digital evidence, and the chain of custody. The module covers evidence acquisition and imaging, hashing and verification, file system analysis, recovery of deleted files, and analysis of operating system artefacts such as logs and the registry. Students also study memory forensics, network forensics, e-mail and browser forensics, and an introduction to mobile device forensics. Anti-forensic techniques and report writing for legal proceedings are discussed. Laboratory sessions use professional forensic tools to acquire and analyse evidence from realistic case scenarios.			

Module 49

Code	Course/Module Title	ECTS	Semester
CYBS-410	Intelligent Analysis of Security Threats	4	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module applies artificial intelligence and data analysis techniques to the detection and analysis of security threats. Students study security data sources, including network traffic, system logs, and malware samples, and the preparation of security datasets and feature extraction. The module covers machine learning methods for intrusion detection, anomaly detection, malware classification, and phishing and spam detection, together with model evaluation using appropriate metrics. Students are introduced to deep learning in security, threat intelligence, and the risks of adversarial attacks against learning models. Tutorial sessions involve analysing public security datasets and discussing research papers in the field.			

Module 50

Code	Course/Module Title	ECTS	Semester
CYBS-411	Information Risk Management	4	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	2 / - / - / 1	48	52
Description			
This module teaches students how organisations identify, assess, and manage information security risks. Students study risk concepts, the risk management process, and the relationship between assets, threats, vulnerabilities, and impacts. The module covers qualitative and quantitative risk assessment methods, recognised standards and frameworks such as ISO/IEC 27001, ISO/IEC 27005, and the NIST risk management framework, and the selection of risk treatment options and security controls. Students also study business continuity and disaster recovery planning, information security governance, policies, and compliance. Tutorial sessions require students to carry out a risk assessment for a case-study organisation and prepare a risk treatment plan.			

Module 51

Code	Course/Module Title	ECTS	Semester
CYBS-412	Project II	7	8
Class (hr/w)	Lect/Lab./Prac./Tutor	SSWL (hr/sem)	USWL (hr/sem)
3	- / - / 3 / -	47	128
Description			
This module is the second part of the graduation research project and completes the work begun in Project I. Under the supervision of a faculty member, students fully implement their proposed solution, whether a security tool, a system, an analysis, or an experimental study. They test and evaluate the solution using suitable methods and metrics, compare their results with related work, and discuss limitations and future work. Students write a complete graduation project thesis according to the department's guidelines, and present and defend their work before an examination committee. The module integrates the knowledge and skills gained throughout the program and demonstrates students' readiness for professional practice or postgraduate study.			

3. Contact

Program Manager:

Dr. Oday Hashim Saeed Al-Wattar | Ph.D. | Assistant Prof. | Head of the Department of Cyber Security

Program Coordinator:

Dr. Faris Adel Hamed | Ph.D.

Address:

Department of Cyber Security, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq.