Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Al-Farabi
Department of Cyber Security Science

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة الفارابي
قسم علوم الامن السيبراني

دليل البرنامج الدراسي
2025-2024
Program Catalogue

Table of Content:

1. Mission & Vision Statement

The Cyber Security Department's vision is to become a global leader in the field, driving the advancement of knowledge, innovation, and best practices to create a safer and more resilient digital world. We are dedicated to achieving excellence in all aspects of Cyber Security, from cutting-edge research and education to practical solutions that safeguard individuals, organizations, and nations against Cyber threats. Our commitment to continuous learning, innovation, and collaboration sets us on a path to address the ever-evolving challenges of the digital age. We aspire to be at the forefront of shaping the future of Cyber Security, making a positive and lasting impact on the security and integrity of digital environments worldwide.

Mission Statement

Our department mission is to educate, innovate, and secure. We educate the next generation of Cyber Security professionals, fostering a deep understanding of Cyber threats and defenses. We innovate through cutting-edge research, developing solutions that anticipate and mitigate emerging risks. We secure individuals, organizations, and society at large by delivering actionable expertise and empowering informed decision-making. With unwavering commitment, we strive to create a resilient digital world that enables trust and prosperity in the digital age.

2. Program Specification

Programme code:	BSc-CYS	ECTS	240
Duration:	4 levels, 8 Semesters	Method of Attendance:	Full Time

Program Duration: Typically, a 4-year undergraduate program.
Program Structure:
Full Time Foundation Level (Year 1-2): The initial years focus on building a solid foundation in Cyber security principles, including network security, cryptography, and ethical hacking. Students acquire essential skills in programming, system administration, and risk assessment.

Advanced Levels (Year 3-4): In the later years, students delve deeper into specialized areas of Cyber security, such as digital forensics, threat detection and mitigation, and security policy development. Advanced coursework includes hands-on labs, research projects, and practical simulations.

3. Program Objectives

1- Prepare Skilled Professionals: The program aims to prepare graduates with the knowledge, skills, and expertise required to excel as Cyber security professionals in a variety of roles, including Cyber security analysts, ethical hackers, security consultants, and digital forensics experts.

2- Address Industry Demands: The program is designed to align with industry demands and evolving Cyber threats. It seeks to produce graduates who can meet the changing needs of organizations and adapt to emerging technologies and vulnerabilities.

3- Promote Ethical Conduct: One of the program's objectives is to instill a strong sense of ethical conduct and responsible Cyber behavior in graduates. Students are encouraged to adhere to ethical hacking practices and uphold the highest standards of integrity in the field.

4- Foster Critical Thinking: The program aims to foster critical thinking and problem-solving skills in students. Graduates should be capable of analyzing complex Cyber security challenges, identifying vulnerabilities, and devising effective solutions.

5- Encourage Research and Innovation: The program encourages research and innovation in the field of Cyber security. Students are motivated to engage in research projects that contribute to the body of knowledge and address pressing Cyber security issues.

6- Develop Effective Communication: Effective communication is a key objective of the program. Graduates should be able to communicate Cyber security concepts, findings, and recommendations clearly and persuasively to diverse audiences, including technical and non technical stakeholders.

7- Cultivate Adaptability: The program recognizes the dynamic nature of the Cyber security landscape. Graduates should possess the adaptability and agility to stay current with emerging threats, technologies, and best practices throughout their careers.

8- Promote Professionalism: Graduates are expected to exhibit professionalism in their interactions with colleagues, clients, and organizations. They should prioritize the protection of digital assets, privacy, and compliance with relevant laws and regulations.

9- Facilitate Career Advancement: The program's objective is to facilitate the career advancement of graduates within the Cyber security field. Whether entering the workforce or pursuing advanced degrees, graduates should be well-positioned for success.

10- Contribute to Cyber Resilience: Ultimately, the program seeks to contribute to the Cyber resilience of organizations and society as a whole by producing Cyber security professionals who can effectively safeguard digital ecosystems and respond to Cyber threats.

4. Student Learning Outcomes

Upon completing the Bachelor of Science in Cyber Security program, students will have achieved the following learning outcomes:

1- Comprehensive Cyber Security Knowledge: Graduates will possess a deep understanding of Cyber security principles, including threat modeling, risk assessment, and vulnerability analysis. They will be well-versed in the fundamental concepts that underpin the field.

2- Proficiency in Security Technologies: Students will have acquired proficiency in security technologies, protocols, and tools commonly used in the Cyber security industry. They will be able to effectively implement and manage security measures to protect digital assets.

3- Cyber Threat Identification and Response: Graduates will demonstrate the ability to identify and respond to Cyber threats. They will be skilled in ethical hacking practices, enabling them to proactively assess vulnerabilities and protect systems from attacks.

4- Digital Forensics Expertise: Students will be capable of conducting digital forensics investigations to analyze Cyber incidents, gather evidence, and support legal proceedings. They will have a strong foundation in digital forensic techniques and tools.

5. Security Policy Development: Graduates will be able to develop and implement security policies, procedures, and guidelines that align with industry best practices and compliance requirements. They will contribute to creating a secure organizational environment.

6. Effective Team Collaboration: Graduates will have honed their collaborative skills through team-based Cyber security projects and exercises. They will be adept at working with diverse
teams to address complex security challenges.

7. Ethical and Legal Awareness: Students will demonstrate ethical and legal awareness in Cyber security practices. They will understand the importance of ethical behavior, privacy protection, and compliance with relevant laws and regulations.

8. Research and Practical Skills: Graduates will have acquired research and practical skills through engagement in real-world Cyber security challenges and research projects. They will be capable of applying their knowledge to solve practical Cyber security problems.

9. Effective Communication: Students will possess strong communication skills, enabling them to convey complex Cyber security concepts and findings effectively. They will be adept at presenting their ideas and recommendations to diverse audiences.

10. Continuous Learning: Graduates will recognize the dynamic nature of the Cyber security field and will be committed to continuous learning and professional development. They will adapt to emerging threats and technologies.

5.Academic Staff

1) Ali H.Kashmar | Ph.D in Computer Science | Professor
Email: ali.Habib@alfarabiuc.edu.iq
Mobile: +9647736818458

2) Yasmeen F.Aziz
Email: Yasmeen.Fawzi@alfarabiuc.edu.iq
Mobile: +9647731536763

3) Louey F.Hasan
Email: Louay.Falih@alfarabiuc.edu.iq
Mobile: +9647806839399

6. Credits, Grading and GPA

Credits

University of Al-Farabi is following the Bologna Process with the European Credit Transfer System (ECTS) credit system. The total degree program number of ECTS is 240, 30 ECTS per semester.

1 ECTS is equivalent to 25 hrs student workload, including structured and unstructured workload.

Grading

Before the evaluation, the results are divided into two subgroups: pass and fail. Therefore, the results are independent of the students who failed a course. The grading system is defined as follows:

GRADING SCHEME مخطط الدرجات

Group	Grade	التقدير	Marks (%)	Definition
Success Group (50 - 100)	A - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	FX – Fail	راسب - قيد المعالجة	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note:				
Number Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.				

Calculation of the Cumulative Grade Point Average (CGPA)
The CGPA is calculated by the summation of each module score multiplied by its ECTS, all are divided by the program total ECTS. CGPA of a 4-year B.Sc. degree: CGPA = [(1st module score x ECTS) + (2nd module score x ECTS) + ……] / 240 .

7. Modules

Semester 1 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS101	Programming Fundamentals I	79	96	7		
CYS102	Discrete Structures	64	61	5		
CYS103	Computer Organization	64	61	5		
CYS104	Data Security Principles	79	46	5		
CYS105	English Language I	33	42	3		
CYS 106	Calculus	64	61	5		

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS107	Programming Fundamentals II	79	96	7		
CYS108	Digital Logic Design	79	63	5		
CYS 109	CYSer Security Principles	49	76	5		
CYS 110	Coding & Information Theory	64	36	4		
CYS 111	English Language II	33	42	3		
CYS 112	Probability and Statistics	64	86	6		

Semester 3 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 201	Object Oriented Programming I	77	98	7		
CYS 202	Data Structures	77	73	6		
CYS 203	Computation Theory	62	63	5		
CYS 204	Database Basics	77	73	6		
CYS 205	Stream Cipher	77	73	6		

Semester 4 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 206	Object Oriented Programming II	77	98	7		
CYS 207	Object Oriented Programming II	77	73	6		
CYS 208	Distrbuted Database	77	48	5		
CYS 209	Software Design Security	77	73	5		
CYS 210	Information and Data Security	77	73	5		

Semester 5 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 301	Public Key	77	48	5		
CYS 301	Cloud Computing Principles	47	53	4		
CYS 303	Computer Networks	77	73	6		
CYS 304	Malicious Codes	77	48	5		
CYS 305	CYSer Security Programing	62	63	5		
CYS 306	Artificial Intelligence	77	48	5		

Semester 6 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 307	Smart Search Methods	77	73	6		
CYS 308	Compiler Design	77	48	5		
CYS 309	Mobile and Network Security	47	53	4		
CYS 310	Block Cipher	62	63	5		
CYS 311	Authorization and Access Control	77	48	5		
CYS 312	Secure Communication Protocols	47	78	5		

Semester 7 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 401	Operating Systems	94	56	6		
CYS 402	Internet of Things Security	64	61	5		
CYS 403	Static Websites Programming	94	56	6		
CYS 404	Electronic Security Governance	79	71	6		
CYS 405	Cloud Computing Security	79	96	7		
CYS 406	Graduation Project I	62	88	6		

Semester 8 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS 407	Operating Systems Security	94	56	6		
CYS 408	Dynamic Websites Programming	94	56	6		
CYS 409	Digital Forensics	63	62	5		
CYS 410	E-Commerce and its Security	63	62	5		
CYS 411	Information Risk Management	63	62	5		
CYS 412	Graduation Project II	32	43	3		

8.Contact

Program Manager:
Ali H.Kashmar
Email: ali.Habib@alfarabiuc.edu.iq
Mobile: +9647736818458

Program Coordinator:
Yasmeen F.Aziz
Email: Yasmeen.Fawzi@alfarabiuc.edu.iq
Mobile: +9647731536763