

جامعة الفلوجة

University of Fallujah



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



1. Table of Contents

1. Mission & Vision Statement
2. Program Specification
3. Program (Objectives) Goals
4. Program Student learning outcomes
5. Academic Staff
6. Credits, Grading and GPA
7. Modules
8. Contact

2. Mission & Vision Statement

Vision Statement

To achieve excellence in cybersecurity education and research by empowering the next generation of professionals with rigorous academic preparation, practical experience, and innovative skills to build and secure national digital infrastructures and contribute to global cyber-defense advancements.

Mission Statement

To prepare a generation of specialists capable of building, securing, and advancing robust digital infrastructures, networks, and systems, and responding to evolving cyber threats through comprehensive academic programs that integrate theoretical education, practical training, and innovation in applied research. The department also seeks to strengthen the university's role in serving the Iraqi and global community by providing sustainable technical solutions, fostering research partnerships, and delivering specialized services that meet growing needs.

3. Program Specification

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

Cybersecurity is a multidisciplinary and rapidly evolving field concerned with protecting digital systems, networks, software, data, and critical information infrastructures from

cyber threats, vulnerabilities, and malicious activities. The Bachelor of Science (B.Sc.) in Cybersecurity at the University of Fallujah is designed to equip students with a strong foundation in computer science and cybersecurity while developing the practical skills required to secure modern computing environments and respond to emerging cyber challenges.

The program begins at Level 1 with fundamental studies in computing, programming, mathematics, computer systems, data security, networking, and cybersecurity fundamentals. Students develop essential analytical and technical skills through courses in structured programming, digital logic design, computer systems and applications, probability and statistics, discrete mathematics, and linear algebra and number theory.

At Level 2, students build core competencies in software development, data structures, computer networks, cryptography, databases, web technologies, computation theory, algorithms, and software security. These subjects provide the theoretical and practical foundations necessary for advanced cybersecurity studies and secure software engineering.

Levels 3 and 4 focus on specialized and advanced cybersecurity domains. Students study operating systems, advanced cryptography, network security, secure communication protocols, penetration testing, cloud computing, cryptanalysis, malware and vulnerability analysis, digital forensics, operating systems security, mobile and network security, steganography and watermarking, Internet of Things security, blockchain technology, and artificial intelligence applications in cybersecurity. The curriculum also includes elective specialization areas such as machine learning for cybersecurity and mobile applications development.

The program emphasizes the integration of theoretical knowledge with extensive laboratory work, practical exercises, project-based learning, and the use of industry-standard cybersecurity tools and platforms. Students gain hands-on experience in secure software development, system hardening, vulnerability assessment, digital investigation, and cyber defense operations. Through research methodology studies and a capstone graduation project, students develop advanced analytical, problem-solving, communication, and research skills that prepare them for professional careers, industry certifications, and postgraduate studies in cybersecurity and related fields.

4. Program Objectives

1. **Provide high-quality academic education** that builds strong theoretical foundations and practical skills in cybersecurity, aligned with international standards and labor-market requirements.

2. **Strengthen hands-on learning and professional readiness** by integrating laboratory work, simulation environments, and applied training scenarios into the curriculum.
3. **Prepare qualified graduates** capable of designing, building, securing, developing, and managing digital infrastructures, computer networks, and critical information systems across public and private sectors.
4. **Develop independent and lifelong learning skills** by encouraging students to explore emerging technologies, monitor evolving cyber threats, and continuously enhance their professional competencies.
5. **Promote applied and innovative research** in cybersecurity, digital forensics, secure systems, and emerging cyber technologies, contributing to national and global knowledge advancement.
6. **Foster ethical, responsible, and professional cybersecurity practices**, and support engagement with governmental institutions and local and international industry to enhance societal awareness and professional relevance.

5. Student Learning Outcomes

Upon successful completion of the program, graduates will be able to:

Outcome 1 - *Cybersecurity Knowledge*

Demonstrate a solid understanding of core cybersecurity concepts, including data security, cryptography, network security, operating systems security, software and applications security, and secure communication protocols.

Outcome 2 - *Technical and Practical Skills*

Apply practical skills and modern tools to design, build, and secure systems, analyze vulnerabilities, perform penetration testing, and implement appropriate security controls.

Outcome 3 - *Analytical and Critical Thinking*

Analyze complex cybersecurity problems, evaluate risks, and propose effective technical solutions based on scientific and engineering principles.

Outcome 4 - *Secure Systems and Networks*

Design, build, configure, and manage secure computer systems, networks, and applications in accordance with best practices and recognized security standards.

Outcome 5 - *Ethical and Professional Responsibility*

Demonstrate awareness of ethical, legal, and professional responsibilities in cybersecurity practice and comply with relevant laws and regulations.

Outcome 6 - *Communication and Teamwork*

Communicate cybersecurity concepts, analyses, and solutions effectively in written and oral forms, demonstrate independent learning and information-seeking skills, and work efficiently within multidisciplinary teams.

6. Academic Staff

#	Full name	Major	Specialization	Email
1.	Asst. Prof. Dr. Omar Salah Farhan Shareef	Computer Science	Data security	omar.alshareef@uofallujah.edu.iq
2.	Lect. Dr. Ahmad Abduljabbar Hamad Alsabhany	Computer Science	Data security	ahmad.alsabhany@uofallujah.edu.iq
3.	Lect. Dr. Senan Ali Abd Dally	Computer Science	Networking	senan.a.abd@uofallujah.edu.iq
4.	Lect. Dr. Omar Abdulmaged Hammood Ali	Computer Science	Networking	omer.abd@uofallujah.edu.iq
5.	Lect. Dr. Ahmed Hadi Ali Farhan	Computer Science	Cloud computing	Ahmed_hadi@uofallujah.edu.iq
6.	Lect. Dr. Mohammed Abduljawad Mohammed Al-shibly	Communications Engineering	wireless communications	mohammed.abduljawad@uofallujah.edu.iq
7.	Lect. Osamah Muzahem Abduljabbar Hassan	Computer Engineering	Cloud computing networks	almihamdi@uofallujah.edu.iq
8.	Lect. Bassim Muhammed Saleh	Computer Science	Information Systems and Technology	Bassim.M.S1977@uofallujah.edu.iq
9.	Lect. Omar Dhafer Madeh	Computer Science	Information Systems	omar.dhafer@uofallujah.edu.iq
10.	Asst. Lect. Mufeed Hameed Saleh Mubark	Computer Engineering	Artificial Intelligence Engineering	mufeed.h@uofallujah.edu.iq
11.	Asst. Lect. Omar Waleed Jawad	Computer Engineering	Networking	omar.waleed@uofallujah.edu.iq
12.	Asst. Lect. Ammar Hatem Farhan	Computer Science	Information System	cs.20.52@uofallujah.edu.iq
13.	Asst. Lect. Raad Muakhlef Khalefa	Computer Science	Information Systems	raad.muakhlef@uofallujah.edu.iq
14.	Asst. Lect. Rawa Sadi Ibrahim	Civil Engineering	Construction	rawa.s.ibrahim@uofallujah.edu.iq

7. Credits, Grading and GPA

Credits

The University of Fallujah follows the Bologna Process using the European Credit Transfer System (ECTS). The total credit requirement for the Bachelor of Science in Cybersecurity is 240 ECTS, distributed as 30 ECTS per semester. One ECTS corresponds to 25 hours of total student workload, including structured and unstructured learning activities.

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:

Group	Grade	Marks (%)	Definition
Success Group (50 - 100)	A - Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 - 49)	FX - Fail	(45-49)	More work required but credit awarded
	F - Fail	(0-44)	Considerable amount of work required
Note:			

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:

$$\text{CGPA} = [(1\text{st module score} \times \text{ECTS}) + (2\text{nd module score} \times \text{ECTS}) + \dots] / 240$$

8. Curriculum/Modules

Semester 1 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS101	Structured Programming I	78	122	8	B	
CYS133	Discrete Mathematics	78	72	6	C	
CYS109	Data Security Principles	48	77	5	C	
CYS103	Mathematics	78	97	7	B	
UFall113	Democracy and Human rights	32	18	2	S	
UFall111	English language I	32	18	2	S	

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS111	Structured Programming II	78	122	8	B	
CYS107	Computer Networks Fundamentals	78	72	6	C	
CYS108	Cybersecurity Fundamentals	78	79	7	C	
CYS105	Digital Logic Design	63	62	5	C	
CYS113	Probability and Statistics	32	18	2	B	
UFall120	Arabic language I	32	18	2	S	

Semester 3 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS201	Object Oriented Programming I	78	47	5	B	
CYS205	Data Structures	63	62	5	C	
CYS217	Computer Networks	78	72	6	C	
CYS229	Cryptography	78	72	6	C	
CYS231	Web Design	63	37	4	C	
UFall225	English language II	32	18	2	S	
UFall211	Ba'ath Regime Crimes	32	18	2	S	

Semester 4 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS211	Object Oriented Programming II	78	47	5	B	
CYS225	Analysis & Design of Algorithms	78	47	5	C	
CYS261	Web Application Development	63	62	5	C	
CYS213	Computation Theory	48	52	4	C	
CYS251	Database Management Systems	63	62	5	C	
CYS258	Software Security	63	37	4	C	
UFall224	Arabic Language II	32	18	2	S	

Semester 5 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS339	Advanced Cryptography	78	97	7	C	
CYS325	Operating Systems	78	72	6	C	
CYS337	Secure Communication Protocols	63	37	4	C	
CYS338	Penetration Testing I	78	72	6	C	
CYS391	Open Source Web Development	63	62	5	C	
CYS304	Hacking Ethics and Laws	33	17	2	B	

Semester 6 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS349	Cryptanalysis	78	72	6	C	
CYS317	Cloud Computing	48	27	3	C	
CYS378	Network Security	78	72	6	C	
CYS348	Penetration Testing II	78	72	6	C	
CYS335	Coding & Information Theory	63	62	5	C	
CYS316	Artificial Intelligence	63	37	4	E	

Semester 7 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS498	Malware & Vulnerability Analysis	78	97	7	C	
CYS478	Mobile & Network Security	78	72	6	C	
CYS486	Machine Learning for Cybersecurity	63	62	5	E	
CYS419	Digital Forensics	63	62	5	C	
CYS439	Steganography & Watermarking	63	62	5	C	
CYS404	Research Methodology	32	18	2	C	

Semester 8 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYS487	Internet of Things Security	63	62	5	C	
CYS449	Blockchain Technology	63	37	4	C	
CYS441	Mobile Applications Development	63	62	5	E	
CYS459	Authentication and Access Control	78	72	6	C	
CYS418	Operating Systems Security	78	72	6	C	
CYS414	Graduation Project	47	53	4	C	

9. 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
