Al-karkh University of Science
جامعة الكرخ للعلوم

First Cycle – Bachelor's degree (B.Sc.) – Cybersecurity Engineering

بكالوريوس علوم - هندسة الأمن السيبراني

Table of Contents | جدول المحتويات

1. Mission & Vision Statement

Vision Statement

To be a leading Cybersecurity Engineering program in Iraq and the region, recognized for academic excellence, applied innovation, and impactful research that strengthens the security and resilience of digital systems and critical infrastructure, while preparing highly qualified graduates who contribute to national and global cyber defense.

Mission Statement

- The Cybersecurity Engineering Program is committed to delivering rigorous, engineering-driven education and training that integrates foundational computing, secure system design, and modern cybersecurity practices. The program aims to:
- Prepare competent and ethical cybersecurity engineers capable of designing, building, and operating secure digital systems.
- Develop strong analytical and practical skills in threat modeling, vulnerability assessment, secure software and network engineering, digital forensics, and incident response.
- Promote research, innovation, and entrepreneurship to address real-world cybersecurity challenges across government, industry, and critical sectors.
- Strengthen partnerships with stakeholders to align learning outcomes with labor-market needs and international professional standards.
- Foster a culture of integrity, privacy protection, risk management, and lifelong learning to support sustainable digital transformation.

2. Program Specification

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

Cybersecurity Engineering is a broad and rapidly evolving discipline that integrates computing, networking, electronics, risk management, and secure system design to protect modern digital infrastructure. With a multidisciplinary teaching team, the College of Engineering is well positioned to deliver a program that balances strong theoretical foundations with intensive hands-on practice across hardware, software, and networked environments. The emphasis of the program is on building secure and trustworthy systems end-to-end—covering threats, vulnerabilities, cryptography, secure architectures, digital investigation, governance, and defensive operations aligned with real-world cyber risk.

The program appeals to students for different reasons: for some, the wide range of cybersecurity applications (from enterprise networks to cloud, IoT, and critical infrastructure) is especially attractive, while for others it provides a pathway toward specialization in areas such as network defense, digital forensics, penetration testing, secure software, malware analysis, and security management. Students are supported with a strong foundational stage that enables informed progression into specialized modules as their interests and strengths develop, while maintaining the engineering mindset required to design and evaluate secure solutions.

Level 1 introduces students to essential principles that underpin cybersecurity engineering, including mathematics, programming, computer fundamentals, digital logic, physics/electronics foundations, and introductory networking. Alongside technical skills, students develop awareness of professional responsibility, ethics, and human rights perspectives that are increasingly important in cybersecurity practice (privacy, misuse, and lawful/ethical constraints). This level is designed to support progression into all pathways within cybersecurity and related engineering programs by building confidence in analytical problem solving and practical lab work.

At Level 2, program-specific core topics are introduced more explicitly, strengthening competence in networking, operating systems concepts, secure computing fundamentals, and applied engineering skills that support security analysis and implementation. Students begin to work with security tools and structured methodologies, learning how real systems fail and how defenses are designed, configured, and tested. This stage prepares students for research-informed and application-oriented

specialist modules at Levels 3 and 4, and for tackling realistic security scenarios through team-based and individual technical work.

From Levels 2 to 4, students can typically choose a proportion of their modules, provided that their selections reflect the integrated nature of cybersecurity—from foundations such as algorithms, systems, and data handling, through networks and embedded platforms, to security operations, assurance, and incident response. This flexibility allows students to develop individualized academic pathways while maintaining the breadth of knowledge expected of a cybersecurity engineering graduate. Module choices are made with academic guidance to ensure coherence, progression, and alignment with career goals.

A strong research and innovation ethos is embedded throughout the program through laboratory work, programming assignments, security case studies, design projects, and tutorials that emphasize problem solving under realistic constraints. Practical components are integrated within lecture-based modules and reinforced through dedicated labs where students learn to analyze threats, apply secure configuration, implement cryptographic and defensive techniques, and document findings professionally. At the final level, all students undertake an independent graduation project that may involve secure software development, digital forensics, network defense design, security evaluation, simulation, or experimental research.

Academic tutorials and skills development are supported through structured activities focusing on essential engineering competencies such as technical writing, research methods, teamwork, ethics, and professional presentation, delivered in ways that connect directly to cybersecurity contexts. Students are guided to build strong documentation habits (reports, threat models, test results, and risk assessments) that match professional expectations. This continuity of academic support helps students transition from foundational learning to advanced independent work and prepares them for professional certification pathways and lifelong learning.

The program also seeks to provide opportunities for industrial training and external engagement, subject to availability, enabling students to experience real security environments and understand workplace practices, standards, and compliance requirements. Where possible, students may access seminars, guest lectures, and industry-informed content to strengthen employability and professional awareness. Graduates are prepared for roles in cybersecurity engineering and operations, further postgraduate study, or innovation-driven careers supporting secure digital transformation across government, industry, and critical services.

3. Program Goals

1. Providing Outstanding Educational Programs: Deliver high-quality education in cybersecurity engineering that equips students with strong foundations and advanced practical skills in areas such as network security, secure systems, cryptography fundamentals, digital forensics, and security operations, preparing them for professional practice and lifelong learning.

2. Research and Development: Establish the department as an active center for research and innovation in cybersecurity, including threat detection, secure architectures, cyber-physical and IoT security, incident response, privacy, and resilience, with outcomes that improve the security of national and organizational digital infrastructure.

3. Building Ethical, Responsible Cyber Professionals: Promote responsible and lawful cybersecurity practice by strengthening student understanding of ethics, privacy, human rights, and professional standards, ensuring graduates can balance security objectives with societal and legal responsibilities.

4. Fostering Industrial and Academic Collaboration: Develop strong partnerships with local and international industry, government, and academic institutions to exchange expertise, deliver joint projects, enhance curriculum relevance, and provide practical training, internships, and employment pathways for students and graduates.

5. Developing Practical Security Applications: Encourage the development of real-world cybersecurity solutions that address modern challenges such as ransomware defense, secure networking, identity and access management, secure software and web systems, cloud security, and protection of critical services through applied projects and laboratories.

6. Promoting Awareness and Contributing to Society: Raise cybersecurity awareness through workshops, competitions, seminars, and community initiatives that educate the public on safe digital behavior, privacy protection, and cyber risk, while supporting community and institutional resilience against cyber threats.

7. Developing National Capabilities: Prepare national talent capable of strengthening Iraq’s cybersecurity capacity by producing graduates who can protect organizations, support digital transformation, contribute to policy and compliance needs, and help grow the knowledge economy through secure and trusted technology adoption.

4. Student Learning Outcomes

Outcome 1 – Engineering Knowledge

Graduates will be able to apply knowledge of mathematics, computer science, networking, and electronics/engineering principles to analyze and solve complex problems in cybersecurity systems and digital infrastructure.

Outcome 2 – Problem Analysis

Graduates will be able to identify, formulate, and analyze complex cybersecurity problems involving threats, vulnerabilities, attacks, and risk using appropriate analytical, computational, and evidence-based methods.

Outcome 3 – Secure System Design

Graduates will be able to design and implement secure systems, networks, and applications that meet specified technical, functional, safety, and regulatory constraints, including privacy, ethics, and sustainability considerations.

Outcome 4 – Security Experimentation and Data Analysis

Graduates will be able to plan and conduct security experiments and investigations, collect and analyze security data (logs, traffic, artifacts), and interpret results to support detection, response, and improvement of defenses.

Outcome 5 – Modern Engineering Tools

Graduates will be able to select and use modern cybersecurity and engineering tools, programming environments, testbeds, and simulation/virtualization platforms to develop, assess, and validate secure solutions.

Outcome 6 – Communication Skills

Graduates will be able to communicate effectively, orally and in writing, technical security information, risk assessments, and investigation findings to diverse audiences, including both technical and non-technical stakeholders.

Outcome 7 – Ethics and Professional Responsibility

Graduates will be able to recognize ethical, legal, and professional responsibilities in cybersecurity engineering and evaluate the societal impacts of security decisions, including privacy, fairness, and responsible disclosure.

Outcome 8 – Teamwork and Leadership

Graduates will be able to function effectively as a member or leader of multidisciplinary teams to plan, implement, and manage cybersecurity projects, including incident response and secure system deployment.

Outcome 9 – Lifelong Learning

Graduates will be able to acquire and apply new knowledge as needed, using appropriate learning strategies, to adapt to rapid changes in cyber threats, technologies, standards, and professional practices.

5. Academic Staff

Program Manager:
Ali Abdulwahhab | Ph.D in Assistant Professor | Assistant Professor
Email: ali_abdulwahhab@kus.edu.iq

Mustafa Ayad Anwer| Ph.D. in Computer Networking| Lecturer
Email: mustafa.alani@kus.edu.iq

Omar Kanaan Noori | PhD in electrical and electronic engineering | Lecturer
Email: Omar.k84@kus.edu.iq

Ammar Isam Mohammed| Ph.D. in Electrical and Electronic Engineering| Lecturer
Email: ammarisam@kus.edu.iq

Samer kais Jameel | Ph. D. In Computer Science. | Lecturer
Email: samer.kais@kus.edu.iq

Ahmed Sabri | MSc. In ICT and Communication Systems | Lecturer
Email: eng.ahmed.sabri@kus.edu.iq

Yahya Bsheer Abdullah | Masters in Electrical and Electronic Engineering | Assistant Lecturer
yahya@kus.edu.iq

Marwa Aubied Khioon | Master Degree in Laser Engineering | Assistant Lecturer
Email: marwa.aubied@kus.edu.iq

Hamid Jassam Mohammed | Master Degree of Software Engineering | Assistant Lecturer
Email: hamidj.mohammed@kus.edu.iq

Omar Salam Abdulhafedh| Master of Computer and Communications Engineering| Assistant Lecturer
Email: omer.salam@kus.edu.iq

Eman khalid ibraheem| master in Computers engineering | Lecturer
Email: eman.khalid@kus.edu.iq

Maalim Qasim Mohammed/ Master/ Communication /
Email: maalim.q.mohammed@kus.edu.iq

6. Credits, Grading and GPA

Credits

Al-karkh University of Science 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)

1. 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. Curriculum/Modules

Semester 1 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
KUS11001	Mathematics I	63	62	5.00	B	
KUS11002	Fundamentals of computer science	63	62	5.00	B	
KUS11003	Democracy and Human Rights	33	17	2.00	B	
CEN11004	Engineering Drawing	48	52	4.00	S	
CEN11005	Physics	63	37	4.00	B	
CYE11006	Biology	33	67	4.00	B	
CYE11007	Digital Logic Design	63	87	6.00	C	

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYE12008	Mathematics II	48	52	4.00	B	
CYE11009	Networks Fundamentals	63	62	5.00	C	
KUS12010	Arabic Language I	33	17	2.00	B	
KUS12011	English Language I	33	17	2.00	B	
CYE12012	Electrical Circuits Analysis	63	87	5.00	S	
CYE11014	Cybersecurity Fundamentals	48	77	5.00	C	
CYE11015	Computer Programming	63	112	7.00	C	

8. Contact

Program Manager:
Ali Abdulwahhab | Ph.D in Assistant Professor | Assistant Professor
Email: ali_abdulwahhab@kus.edu.iq

Program Coordinator:
Ahmed Sabri | MSc. In ICT and Communication Systems | Lecturer
Email: eng.ahmed.sabri@kus.edu.iq