Al-Iraqia Science University

جامعة العلوم العراقية

First Cycle – Four Levels – 240 ECTS
Bachelor's Degree (B.Sc.) – Cybersecurity Engineering

الدورة الأولى - بكالوريوس هندسة الامن السيبراني – أربع سنوات – ٢٤٠ وحدة اوربية

Table of Contents | جدول المحتويات

1. Vision & Mission 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 Goals

- Program Goals
- Ensure graduates master fundamental and advanced concepts in biology aligned with Iraqi higher education standards.
- Develop research capabilities through modern laboratory training and field studies.

- Promote understanding of Iraq's rich biodiversity and environmental conservation needs.
- Prepare students for postgraduate studies and professional careers in life sciences.
- Contribute to sustainable development through applied biological research.

3. Program Specification Overview

Program code:	CEN11005	**ECTS**	4
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
This course equips Cybersecurity Engineering students with a solid scientific foundation for understanding the physical principles that underlie electrical and electronic systems used in computing, communications, and security hardware. It begins with essential concepts of physical quantities, units, measurement accuracy, vectors, and dimensional analysis to build disciplined engineering reasoning. The course then covers electric charge and the structure of matter, conservation of charge, and methods of charging bodies. Students study electrostatic forces, electric fields, Coulomb's law, field lines, electric dipoles, and electric potential energy—core topics needed to interpret how devices behave at a fundamental level. The curriculum continues with current electricity, resistance, and Ohm's law, followed by capacitors and their combinations, and an introduction to AC circuit behavior, including inductive and capacitive reactance and basic circuit response. A key component of the course is semiconductors: intrinsic and doped materials, charge carriers, PN junction theory, diode characteristics, and practical diode-based applications such as rectification and voltage regulation. Laboratory activities reinforce safe measurement, component testing, and the connection between theory and real circuits.			

Program code:	CYE11006	**ECTS**	4
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
This course is designed as "Biology for Engineers," tailored to the needs of Cybersecurity Engineering students, particularly in the area of biometrics and protection of biological/biometric data. It introduces fundamental biological concepts that help students understand why biometric traits can be unique, measurable, and security-relevant. The course starts with basic biochemistry, water and biomolecules, then moves to cell structure, membranes, and transport processes. Students learn about enzymes, energy transformation, cellular respiration, and photosynthesis, followed by cell division and inheritance principles. A central component is genetics and DNA: chromosome structure, DNA replication, and the flow of information from DNA to proteins through transcription and translation. These foundations are connected to real biometric modalities such as fingerprints, iris/retina patterns, voice characteristics, gait, and behavioral biometrics (e.g., keystroke dynamics). The course also addresses variability, bias, and fairness considerations in biometric systems. In addition, it emphasizes ethics, privacy, consent, and the security implications of collecting, storing, and processing biometric data—highlighting risks such as spoofing, template leakage, misuse, and identity permanence, and discussing engineering approaches to reduce these risks.			

Program code:	CYE11007	**ECTS**	6
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
Digital Logic Design is a foundational course that develops the digital thinking required to understand and engineer hardware-based systems, embedded platforms, and low-level computing components that underpin many cybersecurity applications. The course begins with an introduction to digital electronics and how digital representation differs from analog signals. Students learn number systems, base conversions, and binary arithmetic, which are essential for understanding internal data representation and machine-level operations. The course then covers logic gates, truth tables, and Boolean algebra, including key laws and theorems used to model and simplify logic functions. A major emphasis is placed on optimization through Karnaugh maps (K-Maps) to reduce circuit complexity, cost, and error probability. Students design and analyze combinational circuits such as adders/subtractors, multiplexers, decoders/encoders, and comparator structures. The course extends to sequential logic: latches and flip-flops, registers, counters, finite-state concepts, and timing considerations such as propagation delay and clocking behavior. Practical work typically includes simulation, verification, and troubleshooting of circuits, helping students build strong skills in systematic design and testing. The course also supports later cybersecurity topics by strengthening understanding of hardware trust, embedded systems behavior, and the foundations of secure hardware/software interaction.			

Program code:	CEN11004	**ECTS**	4
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
Engineering Drawing develops the student's ability to communicate technical ideas precisely through standardized engineering graphics. Although cybersecurity is often viewed as software-centric, cybersecurity engineers increasingly engage with devices, lab environments, embedded systems, and physical infrastructure where accurate technical documentation is essential. This course starts with drawing instruments and correct drafting practices, followed by geometric constructions (lines, circles, tangency, polygons, and curves) that build spatial reasoning and drafting discipline. Students learn technical lettering, line conventions, and dimensioning rules according to recognized standards, enabling drawings that can be interpreted consistently by others. The course then covers orthographic projection—front, top, and side views—to represent three-dimensional objects in two dimensions, and introduces isometric and perspective representations to visualize components more effectively. Sectional views are included to reveal internal features that cannot be seen from external projections, and students may learn the basics of surface development for certain shapes. The course often introduces computer-aided design (CAD) concepts to improve accuracy, speed, and revision capability. By the end, students are able to read and produce complete technical drawings with proper dimensions and conventions—skills valuable for documenting equipment layouts, enclosures, cabling paths, and engineering configurations.			

Program code:	KUS11001	**ECTS**	5
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
This course provides a strong foundation in integral calculus as an essential analytical tool for engineering study and practice. It develops the student's ability to model, compute, and interpret integrals, which appear throughout engineering topics such as physics, signals, systems, control, and performance analysis. The course begins with fundamental integration techniques and builds competence with indefinite integrals and the concept of antiderivatives. Students then study definite integrals and their geometric meaning, including applications such as computing areas under curves and accumulated quantities. The curriculum expands to more advanced techniques, including substitution methods, integration by parts, and partial fraction decomposition—tools needed to solve complex rational and composite integrals. Trigonometric integrals and trigonometric substitutions are also introduced, especially for expressions containing radicals and quadratic forms. The course typically includes improper integrals and convergence ideas, helping students handle infinite intervals or integrands with singularities. Applications are emphasized to connect mathematics to engineering needs, such as calculating volumes of revolution and other measurable physical quantities. Throughout, the course stresses structured problem-solving: selecting the right method, executing computations accurately, checking results, and interpreting the meaning of solutions in real contexts. This mathematical maturity supports later cybersecurity engineering studies involving modeling, analysis, and quantitative reasoning..			

Program code:	KUS11002	**ECTS**	5
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
Fundamentals of Computer Science 1 provides an organized introduction to computing essentials that Cybersecurity Engineering students need for effective study and professional practice. The course begins with core concepts: what a computer is, how hardware and software interact, and how information is represented and processed. Students learn about major computer components—CPU, memory, storage, and input/output devices—along with common peripheral technologies. The course then covers operating systems and graphical user interfaces, including file management, basic system operations, and practical computing workflows. A strong skills component typically includes productivity tools: word processing for technical reports, spreadsheets for data handling and analysis, and presentations for structured communication of technical ideas. Internet fundamentals are introduced, including browsing, search skills, email, and basic awareness of networking concepts such as local and wide-area networks and online collaboration services. The course often includes introductory programming using Python, focusing on basic syntax, input/output, variables, conditions, loops, and simple data structures to develop algorithmic thinking. Importantly for cybersecurity students, the course incorporates initial cybersecurity and digital ethics awareness—safe user behavior, responsible use of technology, and basic concepts relevant to protecting personal and organizational information in everyday computing environments.			

Program code:	KUS11003	**ECTS**	2
Duration:	1 level, 1 Semester	**Method of Attendance:**	Full Time
This course builds legal, ethical, and societal awareness that complements the technical identity of a Cybersecurity Engineering student. Cybersecurity work often intersects with privacy, surveillance, freedom of expression, due process, and the protection of personal data; therefore, understanding human rights concepts strengthens professional responsibility and compliance-minded decision-making. The course introduces the concept, nature, and characteristics of human rights and discusses their historical development, highlighting how modern rights frameworks emerged. It clarifies distinctions between human rights and other categories of rights, and explores the presence of human-rights principles within major religions and cultural traditions. Students examine international and regional human rights instruments, treaties, and declarations, and consider how national legislation and institutions can protect rights through legal guarantees and enforcement mechanisms. The course also addresses accountability: legal consequences, sanctions, and remedies related to rights violations. For cybersecurity students, this context is particularly important when designing or operating systems that process personal information, enable monitoring, support investigations, or implement automated decision-making. By the end, students should be able to connect technical choices to societal impact, evaluate trade-offs between security and rights, and adopt a professional posture that respects human dignity, privacy, and democratic values while meeting legitimate security objectives.			

4. Program Learning Outcomes

4.1 Knowledge and Understanding (K)

K1. Demonstrate comprehensive understanding of core concepts in cybersecurity engineering, including confidentiality, integrity, availability, authentication, authorization, and non-repudiation.

K2. Explain principles of secure software development, operating system security, and secure system architecture.

K3. Describe computer networks, protocols, and network security mechanisms (e.g., segmentation, firewalls, IDS/IPS, VPNs).

K4. Understand cryptographic fundamentals and practical applications (symmetric/asymmetric cryptography, hashing, key management, PKI).

K5. Explain threat landscapes, attacker models, vulnerabilities, and common attack techniques across systems and networks.

K6. Understand risk management, security governance, policies, compliance concepts, and the security lifecycle.

K7. Recognize digital forensics principles, evidence handling, incident response stages, and security monitoring concepts.

K8. Understand ethical, legal, and societal implications of cybersecurity, including privacy and professional responsibilities, within the Iraqi context.

4.2 Intellectual/Cognitive Skills (C)

C1. Apply systematic problem-solving and security thinking (threat modeling, attack surface analysis) to cybersecurity challenges.

C2. Analyze complex security problems, identify root causes, and propose technically sound mitigations.

C3. Design security controls and architectures that balance protection, usability, and performance.

C4. Critically evaluate cybersecurity research, technical reports, advisories, and standards-based documentation.

C5. Synthesize information from multiple sources (logs, alerts, system behavior, documentation) to form coherent security judgments.

C6. Apply quantitative reasoning and basic statistical concepts to interpret security data and trends.

C7. Make evidence-based decisions for risk treatment (avoid, mitigate, transfer, accept) in realistic scenarios.

C8. Demonstrate creative and adversarial thinking to anticipate attacker behavior and improve defensive strategies.

4.3 Practical and Professional Skills (P)

P1. Configure and harden operating systems and network devices using secure baselines and best practices.

P2. Use security tools for monitoring, vulnerability assessment, and basic penetration testing in controlled environments.

P3. Collect, preserve, and analyze digital evidence while maintaining integrity and proper documentation.

P4. Perform incident response tasks: triage, containment, eradication, recovery, and post-incident reporting.

P5. Implement secure coding practices, conduct code reviews, and apply common mitigation techniques (input validation, least privilege, secure authentication).

P6. Deploy and manage cryptographic solutions appropriately (certificates, secure communication, key handling) in practical scenarios.

P7. Produce accurate technical documentation: security reports, risk assessments, and standard operating procedures.

P8. Follow professional ethics, legal constraints, and safety procedures when conducting cybersecurity activities.

4.4 General and Transferable Skills (T)

T1. Communicate cybersecurity concepts and technical findings effectively in English and Arabic, both orally and in writing.

T2. Work effectively in teams, contribute to collaborative tasks, and demonstrate leadership in project settings.

T3. Use information technology tools and productivity platforms to support secure analysis, documentation, and reporting.

T4. Manage time, priorities, and resources to deliver cybersecurity tasks and projects within constraints.

T5. Present technical results to diverse audiences, including non-specialists, with appropriate clarity and structure.

T6. Search, evaluate, and reference technical sources (standards, advisories, documentation) responsibly and accurately.

T7. Demonstrate self-directed learning and professional development aligned with evolving cybersecurity technologies and threats.

T8. Apply structured problem-solving and critical thinking to real-world cybersecurity and engineering scenarios.

5. Academic Staff

Adel Mohammed Salman | Ph.D. in Network Security | Lecturer
Email: adelmsk63@baghdadcollege.edu.iq
Mobile no.: 07810349040

Saif Saad Alamshani | M.Sc. in Information Technology Engineering | Assist. Lect.
Email: saifalamshani@baghdadcollege.edu.iq
Mobile no.: 07736811585

Heba Kahtan Abdul Jabbar | M.Sc. in Computer Science | Assist. Lect.
Email: hibaalmufty@baghdadcollege.edu.iq
Mobile no.: 07875848233

---

6. Credits, Grading and GPA

Credits

Al-Iraqia Science University 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:				

Note: Marks with 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.

ملاحظة: سيتم تقريب العلامات العشرية التي تزيد أو تقل عن ٠.٥ إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، سيتم تقريب علامة ٥٤.٥ إلى ٥٥، بينما سيتم تقريب علامة ٥٤.٤ إلى ٥٤). لدى الجامعة سياسة لا تسمح بـ "حالات الرسوب القريبة من النجاح"، لذا فإن التعديل الوحيد للعلامات الممنوحة من قبل المصححين الأصليين سيكون التقريب التلقائي الموضح أعلاه.

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 module ECTS) + (2nd module score x module ECTS) + (3rd module score x module ECTS) + … + (last module score x module ECTS)] / 240

7. Curriculum/Modules

Semester 1 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
KUS11001	Mathematics I	63	62	5.00	B	
KUS11002	Fundamental 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	

8. Contact

Program Manager:

Adel Mohammed Salman | Ph.D. in Network Security | Lecturer

Email: adelmsk63@baghdadcollege.edu.iq

Mobile no.: 07810349040

Program Coordinator:

Saif Saad Salman | M.Sc. in Information Technology Engineering | Assist. Lect.

Email: saifalamshani@baghdadcollege.edu.iq

Mobile no.: 07736811585

امسح الكود للوصول إلى النسخة الإلكترونية