Republic of Iraq
Ministry of Higher Education & Scientific Research
Supervision and Scientific Evaluation Directorate
Quality Assurance and Academic Accreditation
International Accreditation Dept.

Academic Program Specification Form For The Academic

University: University of Baghdad

College: Al-Khwarizmi College of Engineering

Number Of Departments in the College :

Date of Form Completion:

Dean ’s Name

Date : / /

Signature

Dean ’s Assistant For Scientific Affairs

Date : / /
Signature

The College Quality Assurance And University Performance Manager
Date : / /
Signature

Quality Assurance And University Performance Manager
Date : / /
Signature

TEMPLATE FOR PROGRAMME SPECIFICATION

HIGHER EDUCATION PERFORMANCE REVIEW: PROGRAMME REVIEW

PROGRAMME SPECIFICATION

This Programme Specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the learning opportunities that are provided. It is supported by a specification for each course that contributes to the programme.

1. Teaching Institution	University of Baghdad/Al_Khwarizmi College of Engineering
2. University Department/Centre	Information and Communication Engineering
3. Programme Title	**Cryptography**
4. Title of Final Award	BSc degree in Information and Communication Engineering
5. Modes of Attendance offered	Attendance is Classroom lectures and Electronic learning according to the university rules in 2023-2024
6. Accreditation	Abet
7. Other external influences	
8. Date of production/revision of this specification	2023-2024

9. Aims of the Programme
The course aims to give the student the following subjects: Students will be introduced to classical and modern encryption methods. Also provides the techniques and tool are used to grantee integrity transmission of information on network.

10. Learning Outcomes, Teaching, Learning and Assessment Methods

Knowledge and Understanding

At the completion of the course, students will be able to…

A1. Use classical encryption method to encrypt plaintext and decrypt ciphertext.

A2. Understanding function of Festal Network

A3. Encryption/decryption of the message using Data Encryption Standard (DES) algorithm

A4. Encryption/decryption of the message using Advance Encryption Standard (AES)

A5. Perform confidentially and authentication using public key encryption (RSA)

A6. Encryption/decryption of the message using Stream Cipher (RC4)

B. Subject-specific skills

In addition to the measurable student learning outcomes listed above, students enrolled in cryptography and network security Course will be required to demonstrate their more in-depth knowledge of the course material by

B1. Solving additional, more challenging exam problems.

B2. Assist with mathematical background to understand the complex algorithms.

Teaching and Learning Methods

Lectures, Presentations, Recitation and Documentations

Assessment methods

homework 10%

quizzes - 15%

midterm -15%

final - 60%

C. Affective and value goals

C1. Ability to apply knowledge of mathematics, science and engineering.

C2. Ability to identify, formulate and solve engineering problems.

C3. Ability to use the techniques, skills and modern engineering tools necessary for engineering practice.

.

D. General and Transferable Skills (other skills relevant to employability and personal development)

D1. Ability to design and conduct experiments.

D2. Ability to design a system, component or process to meet desired needs

Teaching and Learning Methods

Lectures, Presentations, Recitation and Documentations

11. Programme Structure				12. Awards and Credits
Level/Year	Course or Module Code	Course or Module Title	Credit rating	
4th		Cryptography		Bachelor Degree Requires (3) credits

11. Course Structure				
Week	Hours	Unit/Module or Topic Title	Teaching Method	Assessment Method
1	3	Introduction, symmetric cipher model, plain text, encryption algorithm.	Class room lecture	Scheduled Quizzes
2	3	Model of conventional encryption cryptography cryptanalysis, block and stream cipher.	Class room lecture	Scheduled Quizzes
3	3	Mono alphabetic substitution ciphers, shift ciphers,	Class room lecture	
4	3	Caesar cipher, the affine cipher	Class room lecture	
4	3	Hill cipher	Class room lecture	
5	3	Playfair cipher	Class room lecture	
6	3	Polyalphabetic ciphers, viginer ciphers	Class room lecture	
7	3	The transposition cipher	Class room lecture	
8	3	Affine cipher , One time pad	Class room lecture	
9	3	Cryptanalysis of symmetric key, Euclid algorithm	Class room lecture	
11	3	Symmetric key algorithms, DES the data encryption standard,	Class room lecture	
12, 13	3	Public key algorithm, RSA, OTHER PUBLIC ALGORITHM		Mid term exam
14, 15	3	Authentication protocol, authentication based on shared secret key, establishing shatred key, the differ Hillman key exchange, authentication using key distribution center, authentication using Kerberos	Class room lecture	

12. Infrastructure	
Required reading: · CORE TEXTS · COURSE MATERIALS · OTHER	Cryptography and Network Security Principles and Practice_ 5th Edition WILLIAM STALLING
Special requirements (include for example workshops, periodicals, IT software, websites)	
Community-based facilities (include for example, guest Lectures , internship , field studies)	Summer training, Scientific visits

13. Personal Development Planning

1. Provide strong foundation in mathematical, scientific and engineering fundamentals necessary to analyze, formulate and solve engineering problems in the field of Information and Communication Engineering.
2. Enhance the skills and experience in defining problems in Information and Communication Engineering design and implement, analyzing the experimental evaluations, and finally making appropriate decisions.

14. Admission criteria .

According to the rules of Ministry of Higher Education and Scientific Research in Iraq.

15. Key sources of information about the programme

1. Books: Cryptography and Network Security by W. Stalling, 5th edition, 2011.
2. Trusted Internet sources related to the Program
3. Papers.

please tick in the relevant boxes where individual Programme Learning Outcomes are being assessed																			
				Programme Learning Outcomes															
Year / Level	Course Code	Course Title	Core (C) Title or Option (O**)**	Knowledge and understanding				Subject-specific skills				Thinking Skills				General and Transferable Skills (or) Other skills relevant to employability and personal development			
				A1	**A2**	**A3**	**A4**	**B1**	**B2**	**B3**	**B4**	**C1**	**C2**	**C3**	**C4**	**D1**	**D2**	**D3**	**D4**
4th		Cryptography		■		■		■	■			■	■	■	■	■			