Course Specification

(Postgraduate Programs)

Course Title:	Applied Cryptography
Course Code:	CE6002
Program:	Master of Science in Computer Engineering
Department:	Computer and Network Engineering
College:	College of Computer
Institution:	Umm Al-Qura University
Version:	2.0
Last Revision Date:	12/4/2025

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)				
2. Course type				
A.	☐University	☐College	☒ Department	☐Track
B.	☐ Required		☒ Elective	
3. Level/year at which this course is offered: (Level 3 or 4)				
4. Course General Description:				
This course focus on advanced topics in the field of applied cryptography, equipping students with a deep understanding of various cryptographic techniques and their real-world applications. Students will recognize modern and advanced standarss and explore the implementation and security implications of zero-knowledge proofs, homomorphic encryption, and elliptic curve cryptography. The course also covers blockchain technologies and their use in decentralized systems, alongside quantum cryptography and its potential impact on modern cryptographic protocols. Through hands-on projects and case studies, students will gain practical experience in designing and assessing cryptographic systems to address emerging security challenges in today's digital landscape.				
5. Pre-requirements for this course (if any)**:**				
Non				
6. Co-requisites for this course (if any)**:**				
Non				
7. Course Main Objective(s):				
To develop a deep understanding of various cryptographic methods, including public-key infrastructures, digital signatures, and advanced encryption standards. To equip students with the skills to implement and critically assess the security of cryptographic systems, including zero-knowledge proofs, homomorphic encryption, and elliptic curve cryptography. To explore and understand the implications of emerging technologies such as blockchain and quantum cryptography in the context of modern security challenges.				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	45	100
2	**E-learning**		
3	**Hybrid** • **Traditional classroom** • **E-learning**		
4	**Distance learning**		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify)……**	
	Total	45

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Identify the fundamentals and modern cryptographic techniques and their applications	K1	Text book reading, Problem solving, Case study	Quiz, Test, Assignment exercises
1.2	Recognize the main emergent cryptography algorithms and technologies like blockchain and quantum cryptography in securing digital communications.	K2		
2.0	**Skills**			
2.1	Apply cryptographic algorithms to design secure systems, ensuring data integrity and confidentiality in various real-world scenarios.	S1 and S2	problem-based learning and flipped classes.	Practical exercises, hands-on mini porjects

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
2.2	Apply new emergent cryotography based technologies such as blockchain	S2	Practical examples and open-ended tasks are used,. Discussion sessions through an online class discussion group to share information and feedback.	
2.3	Analyze and evaluate the security of cryptographic systems, identifying potential vulnerabilities and proposing robust solutions.	S4		
2.4	Communicate effectively through a written report embodying the design, implementation, evaluation of a project in applied cryotography	S3	Project	Project, Report and Presentation
3.0	**Values, autonomy, and responsibility**			
3.1	Appreciate the ethical implications and responsibilities involved in developing and applying cryptographic solutions in protecting privacy and securing information.	V1	Group project and discussion sessions	Written assignments, oral presentations, and design projects. Verbal cross-questioning
3.2	Cultivate a commitment to continuous learning and function effectively on a team as a leader or a team member	V2		

C. Course Content:

No	List of Topics	Contact Hours
1	Shanon's Theory	3
2	Advanced symmetric-key encryption	5
3	Advanced Message integrity techniques	5
4	Advanced Public key Cryptography Techniques	3
5	Authenticated Encryption and Protocols (Identification, Authentication)	5
6	Cryptographic protocols pitfalls and Attacks assumptions	3
7	Secret Key sharing and trusted intermediaries	5
8	Bitcoin & Blockchain	5
9	Quantum computing and post-Quantum Cryptography	5
10	Emerging Trends in applied cryptography	6
Total		**45**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	Midterm Exam	8	20
2	Final Exam	-	20
3	Assignments	Throughout the semester	20
4	Projects	14	30
5	Presentation and report on scientific article(s)	13-14	10

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup, Version 0.6, 2023 https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner, and Ray Perlner, 3nd Edition, Addison-Wesley Professional, 2022, ISBN-10: 0136643604, ISBN-13: 978-0136643609
Supportive References	The instructor may provide as per requirements.
Electronic Materials	The instructor may provide as per requirements.
Other Learning Materials	The instructor may provide as per requirements.

2. Educational and Research Facilities and Equipment Required:

Items	Resources
Facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms
Technology equipment (Projector, smart board, software)	Projector
Other equipment (Depending on the nature of the specialty)	The instructor may provide as per requirements.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students, Program Leaders	Indirect
Effectiveness of students' assessment	Program Leaders	Direct
Quality of learning resources	Students, Faculty	Indirect
The extent to which CLOs have been achieved	Students, Faculty, Program Leaders	Direct and Indirect
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	**Computer and Network Engineering Department Council**
REFERENCE NO.	**The 18th Session Of The Academic Year 1446**
DATE	**15/4/2025**