Course Specification

(Bachelor)

Course Title:	APPLIED CRYPTOGRAPHY
Course Code:	IT460
Program:	IT
Department:	IT
College:	CCIS
Institution:	MAJMAAH UNIVERSITY
Version:	2
Last Revision Date:	31 May 2023 *Pick Revision Date.*

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: 3 (3,0,1)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (9th /5th .....)					
4. Course general Description:					
This course explores modern cryptographic (code making) and cryptanalytic (code breaking) techniques in detail. Topics covered include cryptographic primitives such as symmetric encryption, public key encryption, hashing functions, digital signatures, and message authentication codes, cryptographic protocols, key establishment, Electronic commerce, standard methods of encoding of digital signatures and certificates (X.509), Financial cryptography, payment systems, crypto currencies and bitcoin.					
5. Pre-requirements for this course (if any)**:**					
70 Credits					
6. Pre-requirements for this course (if any)**:**					
7. Course Main Objective(s):					
At the end of the course, the students will be able to: • **Understand and practice the concept of cryptographic algorithms.** • **Learn the current state of the art techniques that are employed for defeating secure systems.** • **Analyze hashing functions, message authentication codes and key establishment** • **Understand Digital signatures in practice with legal/regulatory aspects.** **Understand attacks in payment systems, bitcoin and crypto currencies.**					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100
2	E-learning		
3	Hybrid		

No	Mode of Instruction	Contact Hours	Percentage
	• 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**	15
5.	**Others (specify)**	
Total		60

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

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	CLO1 Understand and practice the concept of cryptographic algorithms	**K1**	Classroom Teaching and Exercise	Test, Mid Exam, Final Exam
2.0	**Skills**			
2.1	CLO2: Learn the current state of the art techniques that are employed for defeating secure systems	**S4 [IT]**	Classroom Teaching and Exercise	Test, Presentation, Mid Exam, Final Exam
	CLO3: Analyze hashing functions, message authentication codes and key establishment	**S1**	Classroom Teaching and Exercise	Test, Presentation, Mid Exam, Final Exam

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	CLO5: Understand attacks in payment systems, bitcoin and crypto currencies	**S2**	Classroom Teaching and Exercise	Test, Presentation, Mid Exam, Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	CLO4: Understand Digital signatures in practice with legal/regulatory aspects	**V2**	Classroom Teaching and Exercise	Test, Mid Exam, Final Exam

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to cryptography, Symmetric cryptography	4
2.	Steam Ciphers and Block Ciphers	4
3---	Data Encryption Standard (DES)	6
4	PKI	4
5	RSA Algorithm	4
6	Diffie-Hellman Key Exchange, El Gamal Encryption Scheme	6
7	Digital Signatures,The RSA Signature Scheme,Digital Signature Algorithm (DSA)	6
8	Cryptographic Hash Functions, Secure Hash Algorithm (SHA)	4
9	Message Authentication Codes, MACs Based on Hash Functions: HMAC	6
10	Key Establishment Using Symmetric and Asymmetric techniques	6
11	Secure Sockets Layer (SSL), Transport Layer Security (TLS)	4
12	Payment Systems	6
Total		**60**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	**Midterm Examination:**	**Week 8**	**20%**
2.	**Class Test**	**Week 4 Week 12**	**20%**

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
3.	Homework/assignments	(as per schedule)	10%
.4	Participation in class		10%
5	Final Examination	Week 16	40%
6	Total		100%

*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	• Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.
Supportive References	• Lindell, Yehuda, and Jonathan Katz. Introduction to modern cryptography. Chapman and Hall/CRC, 2014. ISBN-13: 978-1466570269 • Smart Cards, Tokens, Security and Applications by Keith E. Mayes and Konstantinos Markantonakis. ISBN-13: 978-0-387-72197-2 e-ISBN-13: 978-0-387-72198-9, 2017 Springer Science • W. Stallings, "Cryptography and network security: principles and practice" Pearson; 2017. ISBN-13: 978-0134444284
Electronic Materials	
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classroom
Technology equipment (projector, smart board, software)	PC or Laptop with Windows/Linux, Smart Board, Projector
Other equipment (depending on the nature of the specialty)	Internet Connection

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect
Effectiveness of Students assessment	Instructor	Direct
Quality of learning resources	Instructor	Direct
The extent to which CLOs have been achieved		
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	IT DEPT Council
REFERENCE NO.	
DATE	