هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد NCAAA T4 2020

Course Specifications

Course Title:	Applied Cryptography
Course Code:	IT 461
Program:	IT
Department:	IT
College:	College of Computer and Information Sciences
Institution:	Majmaah University

Table of Contents

A. Course Identification

1. Credit hours: 3
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☐ Elective ☑
3. Level/year at which this course is offered: Track
4. Pre-requisites for this course (if any)**: 70 credits**
5. Co-requisites for this course (if any)**: NIL**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	44	%100
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	33
2	**Laboratory/Studio**	11
3	**Tutorial**	
4	**Others** (specify)	
	Total	44

B. Course Objectives and Learning Outcomes

1. Course 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.

2. Course Main Objectives

At the end of the course, the students will be able to:

1. Learn the current state of the cryptographic approaches used in secure systems.
2. Analyze hashing functions, message authentication codes and key establishment.
3. Understand digital signatures in practice with legal/regulatory aspects.
4. Understand payment systems, bitcoin and crypto currencies.

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge and Understanding**	
1.1		
1.2		
1.3		
1...		
2	**Skills :**	
2.1	CLO1 Understand and practice the concept of cryptographic algorithms	S1
2.2	CLO2: Learn the current state of the art techniques that are employed for defeating secure systems.	S1
2.3	CLO4: Understand Digital signatures in practice with legal/regulatory aspects	S3
2...		
3	**Values:**	
3.1	CLO3: Analyze hashing functions, message authentication codes and key establishment	V2
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to cryptography, Symmetric cryptography	3
2	Steam Ciphers and Block Ciphers	3
3	Data Encryption Standard (DES)	3
4	RSA Algorithm	3
5	Diffie-Hellman Key Exchange, El Gamal Encryption Scheme	3
6	Digital Signatures	3
7	Cryptographic Hash Functions, Secure Hash Algorithm (SHA)	3
8	Message Authentication Codes, MACs Based on Hash Functions: HMAC	3
9	Key Establishment Using Symmetric and Asymmetric techniques	3
10	Secure Sockets Layer (SSL), Transport Layer Security (TLS)	3
11	Payment Systems	3
Total		33

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1			
1.2			
…			
2.0	**Skills**		
2.1	CLO1 Understand and practice the concept of cryptographic algorithms	Classroom Teaching	Class Test, Mid Exam, Final Exam
2.2	CLO2: Learn the current state of the art techniques that are employed for defeating secure systems.	Classroom Teaching	Class Test, Mid Exam, Final Exam
…	CLO4: Understand Digital signatures in practice with legal/regulatory aspects	Classroom Teaching	Class Test, Mid Exam, Final Exam
3.0	**Values**		
3.1	CLO3: Analyze hashing functions, message authentication codes and key establishment	Classroom Teaching	Class Test, Mid Exam, Final Exam
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	Week 5, 10,13	20 %
2	Assignments	Week 7, 13	20%
3	Midterm Exam	Week 8	20 %
4	Final Exam	Week 16	40 %
5			
6			
7			
8			

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :
Each student is allotted to an academic advisor for guidance and counseling.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	• Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.
Essential References Materials	• 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. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom, laboratories
Technology Resources (AV, data show, Smart Board, software, etc.)	PC with Windows/Linux, LCD Projector, Smart Board
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	Internet

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Final Exam Answer Scripts Verification	Review Committee member	Review
Course Feedback	Students	Survey

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	
Reference No.	
Date	