هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA
T4
2020

Course Specifications

Course Title:	**Cryptography**
Course Code:	**501513-3**
Program:	**Bachelor in Computer Science**
Department:	**Department of Computer Science**
College:	**College of Computers and Information Technology**
Institution:	**Taif 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: **15th Level/5**

4. Pre-requisites for this course (if any)**:**

501435-3 and 501324-3

5. Co-requisites for this course (if any)**:**

None

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	5	100
2	**Blended**	0	0
3	**E-learning**	0	0
4	**Distance learning**	0	0
5	**Other**	0	0

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	50
2	**Laboratory/Studio**	
3	**Tutorial**	
4	**Others** (specify)	
	Total	50

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides the students with an understanding of the fundamental concepts of cryptography and cryptanalysis. Starting with classical algorithms (and their cryptanalysis), the focus moves onto the modern cryptographic algorithms, primitives, and infrastructure. This course also provides a brief introduction to mathematical and probabilistic concepts used in cryptographic systems.

2. Course Main Objective

- Students should explain the classical cryptographic algorithms/schemes and analyze their 'hardness'.
- Students should understand different approaches to modern cryptographic algorithms including symmetric key and public key encryption, block and stream ciphers, etc.

Students should understand other primitives, used in modern cryptographic systems, such as digital signatures, digital authentication, digital digests, hash functions, key-exchange protocols, etc.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding:**	
	Describe the classic encryption schemes and their cryptanalysis	K1
2	**Skills:**	
2.1	Apply the related knowledge of mathematics and probability theory to the design and analysis of modern cryptographic algorithms.	S1
2.2	Describe different cryptographic approaches such as symmetric key encryption and asymmetric (public) key encryption and related infrastructure.	S2
2.3	Describe cryptographic primitives such as key exchange, primality testing, zero-knowledge proofs, and so on.	S1
2.4		
3	**Values:**	

C. Course Content

No	List of Topics	Contact Hours
1	Classical encryption algorithms and analyzing their reliability.	5
2	Modular Arithmetic (including Modular Division and subtraction, exponentiation), Properties of Congruences, Euclidean algorithm, basic probability theory, etc.	10
3	Primality Testing: Fundamental Theorem of Arithmetic, Trial Division Test, Fermat’s algorithm, etc. Carmichael numbers, Robin-Miller algorithm, etc.	10
4	Modern cryptography and its features, factoring, one-way functions and their uses	5
5	Symmetric key encryption and DES algorithm	5
6	Public Key encryption: RSA Algorithm and proof, Chinese Remainder theorem, exponentiation by repeated squaring	10
7	Quasi-commutivity and Diffie-Hellman key exchange algorithm	5
	Total	50

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**		
	Describe the classic encryption schemes and their cryptanalysis.	Lectures	**Direct Assessment Tool**

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
			Quizzes / Homework/Excercise/ Exams **Indirect Assessment Tool** Course Exit Survey
2.0	**Skills**		
2.1	Apply the related knowledge of mathematics and probability theory to the design and analysis of modern cryptographic algorithms.	Lectures	**Direct Assessment Tool** Quizzes / Homework/ Exams **Indirect Assessment Tool** Course Exit Survey
2.2	Describe different cryptographic approaches such as symmetric key encryption and asymmetric (public) key encryption and related infrastructure.	Lectures	**Direct Assessment Tool** Quizzes / Homework/ Exams **Indirect Assessment Tool** Course Exit Survey
2.3	Describe cryptographic primitives such as key exchange, primality testing, zero-knowledge proofs, and so on.	Lectures	**Direct Assessment Tool** Quizzes / Homework/ Exams **Indirect Assessment Tool** Course Exit Survey
3.0	**Values**		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Homework/Student Participation-Attendance	Every Week	15%
2	Quizzes	Week 2 and 9	10%
3	Mid-Term	Week 5	25%
4	Final Examination	Week 12	50%

***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:

- 6 hours per week in pre-determined office hours
- Consultation by appointment (as needed)
- Through emails
- Through BlackBoard Learn

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	• Introduction to Modern Cryptography • Jonathan Katz and Yehuda Lindell 2007 CHAPMAN & HALL/CRC
Essential References Materials	None
Electronic Materials	None
Other Learning Materials	None

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	• Classroom with 30 chairs
Technology Resources (AV, data show, Smart Board, software, etc.)	• Video projector / data show • White board
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of Teaching	• Students	Students surveys and Students course evaluation •
Improvement of Teaching	• Course Coordinator	• Deficiencies based on the student Evaluation, faculty input, course file, and program assessment
Verifying Standards of Student Achievement	• Curriculum Committee	• Review CAF (Course assessment file) • Alumni surveys. • Periodic exchange and remarking of tests or a sample of assignments with staff at another

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	CS council
Reference No.	Meeting #12
Date	23-10-1443

قسم علوم الحاسب
Computer Science Department
TU
جامعة الطائف
TAIF UNIVERSITY