Course Specification

(Bachelor)

Course Title:	Cryptography
Course Code:	501513-3
Program:	Bachelor of Computer Science
Department:	Department of Computer Science
College:	College of Computers and Information Technology
Institution:	Taif University
Version:	v1
Last Revision Date:	20-02-2024

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☐Required		☒ Elective		
3. Level/year at which this course is offered: (Level 10 / Year 5)					
4. Course general 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.					
5. Pre-requirements for this course (if any)**:**					
501435-3 Analysis and Design of Algorithms					
6. Co-requisites for this course (if any)**:**					
None					
7. Course Main Objective(s):					
• 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.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	**2**	**67%**
2	E-learning	**1**	**33%**
3	Hybrid • Traditional classroom • E-learning	0	0
4	Distance learning	0	0

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 CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Ability to describe the classic encryption schemes and their cryptanalysis.	**K1**	**Lectures**	**Direct:** Quizzes, Homework, Exams **Indirect:** Course Exit Survey
2.0	**Skills**			
2.1	Ability to apply the related knowledge of mathematics and probability theory to the design and analysis of modern cryptographic algorithms.	**S1**	**Lectures**	**Direct:** Quizzes, Homework, Exams **Indirect:** Course Exit Survey
2.2	Ability to describe different cryptographic approaches such as symmetric key encryption and asymmetric (public) key encryption and related infrastructure.	**S2**	**Lectures**	**Direct:** Quizzes, Homework, Exams **Indirect:** Course Exit Survey
2.3	Ability to describe cryptographic primitives such as key exchange, primality testing, zero-knowledge proofs, and so on.	**S1**	**Lectures**	**Direct:** Quizzes, Homework, Exams **Indirect:** Course Exit Survey
3.0	**Values, autonomy, and responsibility**			

C. Course Content

No	List of Topics	Contact Hours
1	Classical encryption algorithms and analyzing their reliability.	9
2	Modular Arithmetic (including Modular Division and subtraction, exponentiation), Properties of Congruences, Euclidean algorithm, basic probability theory, etc.	6
3	Primality Testing: Fundamental Theorem of Arithmetic, Trial Division Test, Fermat's algorithm, etc. Carmichael numbers, Robin-Miller algorithm, etc.	6
4	Modern cryptography and its features, factoring, one-way functions, and their uses	6
5	Symmetric key encryption and DES algorithm	6
6	Public key encryption: RSA Algorithm and proof, Chinese Remainder theorem, exponentiation by repeated squaring	6
7	Quasi-commutivity and Diffie-Hellman key exchange algorithm	6
Total		45

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1	Homework/Student Participation-Attendance	Every week	15%
2	Quizzes	Week 4 and 12	10%
3	Mid-term	Week 7	25%
4	Final Exam	Week 16	50%

*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	Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell 2007, CHAPMAN & HALL/CRC
Supportive References	
Electronic Materials	
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• Classroom with 30 chairs
Technology equipment (projector, smart board, software)	• Video projector / data show • White board
Other equipment (depending on the nature of the specialty)	

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	• Students • Faculty members • Coordinator • Council • Curriculum Committees	• Course exit survey • Feedback from Faculty members • Feedback from Course Coordinator • Feedback from council • Feedback from Curriculum Committees
Effectiveness of Students assessment	• Students • Faculty members • Coordinator • Council • Curriculum Committees	• Course exit survey • Feedback from Faculty members • Feedback from Course Coordinator • Feedback from council • Feedback from Curriculum Committees
Quality of learning resources	• Students • Faculty members • Coordinator • Council • Curriculum Committees	• Course exit survey • Feedback from Faculty members • Feedback from Course Coordinator • Feedback from council • Feedback from Curriculum Committees
The extent to which CLOs have been achieved	• Students • Faculty members • Coordinator • Council • Curriculum Committees	• Course exit survey • Feedback from Faculty members • Feedback from Course Coordinator • Feedback from council • Feedback from Curriculum Committees
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	CS council
REFERENCE NO.	Meeting #11
DATE	07/03/2024

.