هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024

TP-153

Cryptography

Course Specification
(Bachelor)

Course Title:	Cryptography
Course Code:	CNET 461
Program:	Computer & Network Engineering
Department:	Electrical & Electronics Engineering
College:	College of Engineering & Computer Science
Institution:	Jazan University
Version:	15
Last Revision Date:	22 September 2024

Table of Contents

A. General information about the course: 3

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods 4

C. Course Content 4

D. Students Assessment Activities 5

E. Learning Resources and Facilities 5

F. Assessment of Course Quality 5

G. Specification Approval 6

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: (7/4)					

4. Course General Description:

This course will primarily focus on basic terminology and concepts of cryptography. There are two basic techniques for encrypting information: symmetric encryption and asymmetric encryption. The topics covered in this course includes introduction to cryptography, symmetric and asymmetric cryptography, One time pad, Hill cipher, DES, AES,RC4 ,RSA,DIFFIE-HELLMAN, Man In the Middle Attack, ElGamal Cryptographic System, Elliptic Curve Cryptography and Digital Signatures.

5. Pre-requirements for this course (if any)**:**

MATH 326

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

7. Course Main Objective(s):

This course will develop the students’ ability to learn:

- Understand the fundamentals of Cryptography.
- Describe different types of cryptographic algorithms.
- Analyze and differentiate different types of Cryptographic algorithms
- (Symmetric key and Asymmetric key).
- Analyze appropriate cryptographic algorithms for a given problem.
- Apply cryptographic algorithms to solve specified security problem.
- Calculate public key, private key, plain text, cipher text and digital signatures using different cryptographic algorithms.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	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**	26
2.	**Laboratory/Studio**	26
3.	**Field**	--
4.	**Tutorial**	--
5.	**Others (specify)**	8
Total		60

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	**Describe** basic terminologies, concepts, public key and symmetric key cryptographic algorithms.	K2	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 ● Final Exam
1.2	**Discuss** latest trends and recent developments in the field of cryptography.	K3	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 ● Final Exam
2.0	Skills			

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
2.1	**Differentiate** various types of Symmetric and Asymmetric cryptographic algorithms.	S1	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Assignment 1 ● Mini Project ● Final Exam
2.2	**Implement** different cryptographic algorithms to solve specified security problems.	S2	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Lab Exam ● Mini Project ● Final Exam
2.3	**Evaluate** public key, private key, Plain text and cipher text using different cryptographic algorithms.	S1	● Lectures ● Classroom discussions ● Lab exercises	● Mid-Term Exam ● Lab Exam ● Mini Project ● Final Exam
2.4	**Demonstrate** implementation of different encryption techniques to secure data.	S4	● Lectures ● Classroom discussions ● Lab exercises s	● Mid-Term Exam ● Lab Exam ● Mini Project ● Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	**Perform** self-study and self-assessment through lab assignments.	V2	● Lectures ● Classroom discussions Lab exercises	● Lab Exam ● Mini Project

C. Course Content

No	List of Topics	Contact Hours
1.	**Chapter – 1:** **Introduction of Cryptography** ● **Types of Encryption keys** ● **Stream ciphers and Block ciphers** ● **Caesar Cipher** ● **Hill Cipher** ● **Vernam cipher** ● **One-Time Pad** ● **Transposition Techniques** ● **Shannon's Characteristics of "Good" Ciphers**	4T + 4P
2.	**Chapter – 2: Symmetric Encryption**	4T + 4P

	● Symmetric Encryption ● Vigenere Cipher ● Data Encryption Standard (DES) ● Advanced Encryption Standard (AES) ● DES vs. AES ● Block cipher Mode of operations	
3.	Chapter - 3: BLOCK CIPHER OPERATIONS and STREAM CIPHERS ● Multiple Encryption and DES ● Double DES ● Triple DES with Two Keys ● Triple DES with Three Keys ● Stream ciphers ● Stream cipher Structure ● RC4 STREAM CIPHER ● RC4 Key Schedule ● RC4 Encryption ● RC4 Security	4T + 4P
4.	Chapter - 4: PUBLIC-KEY CRYPTOGRAPHY AND RSA ● Public-Key CRYPTOGRAPHY ● Characteristics of public key encryption ● Keys in symmetric & asymmetric encryption ● RSA Algorithm ● RSA Encryption & decryption ● Comparison between Secret and Public key	4T + 4P
5.	● Chapter – 5: OTHER PUBLIC-KEY CRYPTOSYSTEMS ● Public Key Cryptography to Exchange Secret Keys ● Diffie-Hellman Key Exchange Algorithm ● Diffie-Hellman Example and exercises ● Man in the Middle Attack on DH ● Elgamal Cryptographic System ● Elliptic Curve cryptography	6T + 6P
6.	Chapter – 6: Message digest and Lightweight cryptography ● Message digest and Hash functions ● Message Digests Algorithms ● Message Authentication using Hash Functions ● Digital Signatures ● Lightweight Cryptography Concepts	4T+4P

	● Embedded Systems ● Microcontrollers ● Deeply Embedded Systems ● Constrained Devices ● Categories of Constraints for Lightweight Cryptography ● Profiles of Lightweight cryptography	
7.	Revision all contents	2T+2P
8.	Final Exam	2T + 2P
Total		**60**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	4th Week	10%
2.	Midterm Exam	8th Week	20%
3.	Mini Project	12th Week	10%
4.	Lab Exam	13th Week	20%
5.	Final Exam	15th Week	40%

*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	1. Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies,5th Edition, Prentice Hall, Year- 2015,ISBN 0134085051, 9780134085050 2. Cryptography And Network Security: Principles and practice",William Stallings, 7th Edition, Pearson Education, Year-2017,ISBN 10:1-292-15858-1 , ISBN 13: 978-1-292-15858-7
Supportive References	Cryptography And Network Security, By Behrouz A. Forouzan, 1st edition, McGraw-Hill Education, Year-2010, ISBN-13 : 978-0073327532
Electronic Materials	11. https://lms.jazanu.edu.sa/webapps (Electronic material available in Blackboard to respective groups by each faculty member.) 2. https://www.coursera.org/learn/crypto 3. www.iacr.org
Other Learning Materials	**None**

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	**Classroom equipped with projector and whiteboard and sufficient seating arrangements.** **Lab with software installed and individual computer terminal for each student.**
Technology equipment (projector, smart board, software)	**Whiteboards and projectors for classroom and lab.Following software for lab work:** • **NetBeans IDE 8.2** • **JDK 1.7** • **BlueJ**
Other equipment (depending on the nature of the specialty)	**None**

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	**Students, HOD**	**Indirect, Direct**
Effectiveness of Students assessment	**CT / CC / HoD**	**Direct**
Quality of learning resources	**TL / CRC / PQC**	**Indirect, Direct**
The extent to which CLOs have been achieved	**CT / CC /TL / PQC**	**Indirect, Direct**
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**DEPARTMENT COUNCIL**
REFERENCE NO.	**ENGCSEEE2411**
DATE	**10/10/24**