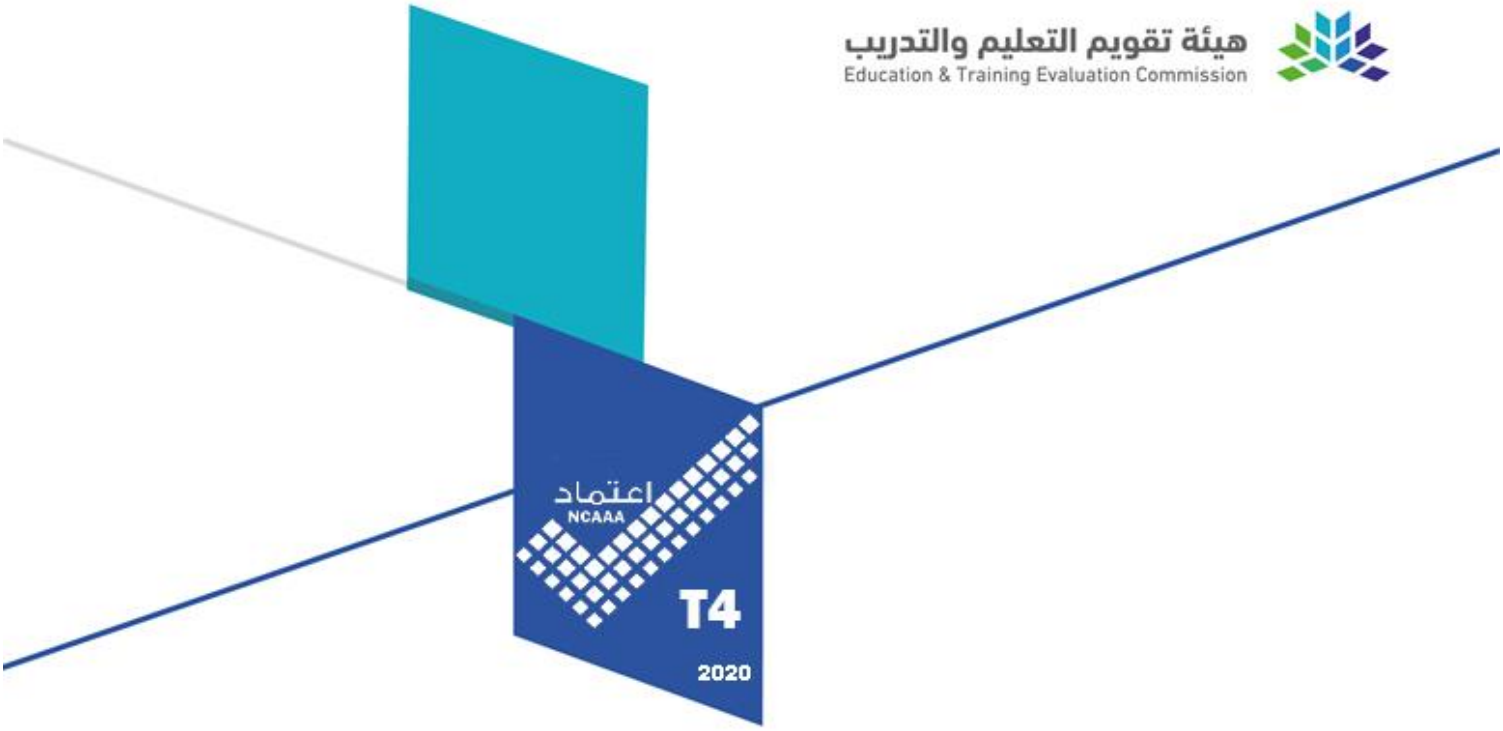
هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Cryptographic Techniques
Course Code:	326 CNET-3
Program:	Bachelor in Computer and Network Engineering
Department:	Computer and Network Engineering
College:	Computer Science and Information Technology
Institution:	Jazan 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: Level-11/Year-04
4. Pre-requisites for this course (if any)**:** Computer Networks (331 CNET-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**	52	100%
2	**Blended**	--	--
3	**E-learning**	--	--
4	**Distance learning**	--	--
5	**Other**	--	--

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	22
2	**Laboratory/Studio**	22
3	**Tutorial**	--
4	**Others** (specify) **Exams and Revision**	8
	Total	52

B. Course Objectives and Learning Outcomes

1. Course 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.

2. Course Main Objective:

- 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.

3. Course Learning Outcomes

	CLOs	Aligned PLOs
1	**Knowledge and Understanding**	
1.1	**Describe** basic terminologies, concepts, public key and symmetric key cryptographic algorithms.	K2
1.2	**Discuss** latest trends and recent developments in the field of cryptography.	K3
2	**Skills :**	
2.1	**Differentiate** various types of Symmetric and Asymmetric cryptographic algorithms.	S1
2.2	**Implement** different cryptographic algorithms to solve specified security problems.	S2
2.3	**Evaluate** public key, private key, Plain text and cipher text using different cryptographic algorithms.	S1
2.4	**Demonstrate** implementation of different encryption techniques to secure data.	S4
3	**Values:**	
3.1	**Perform** self-study and self-assessment through assignments.	V2

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	4T+4P

	• Transposition Techniques • Shannon's Characteristics of "Good" Ciphers	
2	**Chapter – 2:** Symmetric Encryption • Symmetric Encryption • Vigenere Cipher • Data Encryption Standard (DES) • Advanced Encryption Standard (AES) • DES vs. AES • Block cipher Mode of operations	4T+4P
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 • Message digest and Hash functions	6T+6P
	Exams	4T+4P
Total		52

Online Study Topics:
• Message Digests Algorithms • Message Authentication using Hash Functions • Digital Signatures • Properties of Paper-Based & Digital Signatures • Public Keys for Signatures • Cubic equations for elliptic curve Cryptography

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	**Describe** basic terminologies, concepts and public key and symmetric key cryptographic algorithms.	➢ 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.	➢ Lectures ➢ Classroom discussions ➢ Lab exercises	➢ Mid-Term Exam ➢ Mini Project ➢ Assignment1
2.0	**Skills**		
2.1	**Differentiate** various types of Symmetric and Asymmetric cryptographic algorithms.	➢ Lab exercises ➢ Lectures ➢ Classroom discussions	➢ Mid-Term Exam ➢ Final Exam ➢ Mini Project ➢ Assignment 2
2.2	**Implement** different cryptographic algorithms to solve specified security problems.	➢ Lectures ➢ Lab Exercises	➢ Mini Project ➢ Lab Exam ➢ Final Exam
2.3	**Evaluate** public key, private key, Plain text and cipher text using different cryptographic algorithms.	➢ Lectures ➢ Classroom discussion	➢ Mini Project ➢ Lab Exam ➢ Assignment 2 ➢ Final Exam
2.4	**Demonstrate** implementation of different encryption techniques to secure data.	➢ Lectures ➢ Lab exercises	➢ Mini Project ➢ Final Exam ➢ Lab Exam
3.0	**Values**		
3.1	**Perform** self-study and self-assessment through assignments.	➢ Lectures ➢ Classroom discussion	➢ Assignments ➢ Mini Projects

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Assignments / Mini Project	4th Week	20%
2	Midterm Exam	6th Week	20%
3	Lab Exam	11th Week	20%
4	Final Theory Exam	12th Week	40%

***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 :

Department have an arrangement for "Academic Counseling and Support" for each student by the department. The Department Coordinator nominates faculty members for "Student Academic Advisory Committee" every semester. These "Academic Advisors" are responsible for student counseling and advising to a group of fix number of students (around10-15 students) and maintaining students' files. At the beginning of semester and at time of course registration all students take counseling from Academic Advisor according to his previous grades and coverage of pre-requisite course and follow-up.

Also students with GPA below than 2.00 are remained under deep observation and continuous meetings with respective course teachers about their performance are arranged to help and support the students. The course teacher is to be associated with this course provide a proper guidance for students who are looking to focus on their future career based on their intellectual interests, identify better opportunities related to this course and connections in their academic fields.

The course teacher will commit to a minimum scheduled time for student consultation equivalent to *3 HOURS PER WEEK* and will have prescribed times set aside for individual appointments with students. The students will be informed at the commencement of every semester for teacher consultation hours for seeking advice and support.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	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
Essential References Materials	1. Cryptography And Network Security, By Behrouz A. Forouzan, 1st edition, McGraw-Hill Education,Year-2010, ISBN-13 : 978-0073327532 2. Understanding Cryptography, Christof Paar ,Jan Pelzl,Springer, 1st edition,Year-2010, ISBN 978-3-642-04100-6
Electronic Materials	1. 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. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom equipped with projector and whiteboard and sufficient seating arrangements. Lab with software installed and individual computer terminal for each student.
Technology Resources (AV, data show, Smart Board, software, etc.)	Whiteboards and projectors for classroom and lab Following software for lab work: • NetBeans IDE 8.2 • JDK 1.7 • BlueJ
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	None

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Sufficiency of resources and facilities for students	Students	Course evaluation survey form
Effectiveness of teaching / learning process	Students	Course evaluation survey form
Effectiveness of teaching / learning process	CRC / QAU / HoD	Course reports / result analysis
Quality of learning Resources	Track leaders / CRC	Review meetings and star rating with suggestions for further modification and improvements
Verifying standards of student achievement / evaluation	HoD / committee nominated by HoD	Random re-checking of evaluated answer sheets
Achievement of course learning outcomes	Course Teachers / QAU	CLO assessment template that is further verified at course coordinator, Track leader and QAU level.

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	DEPARTMENT COUNCIL
Reference No.	
Date	