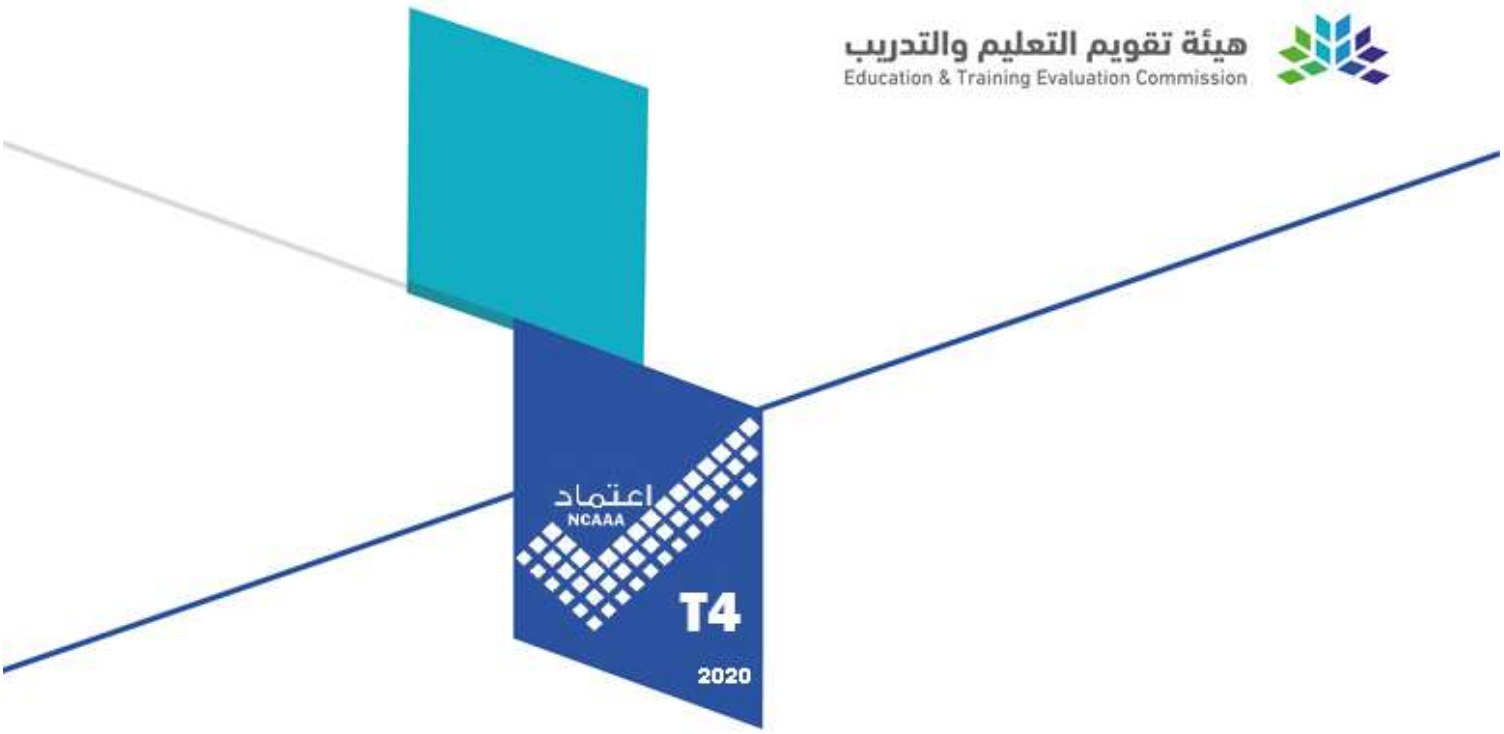
هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Coding and Cryptography Theory	
Course Code:	**MTH 445**	
Program:	**B.Sc in Mathematics**	
Department:	**Mathematics Department**	
College:	**College of Science at Al- Zulfi**	
Institution:	**Majmaah University**	

Table of Contents

A. Course Identification

1. Credit hours: 3(2+1)
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: 7th
4. Pre-requisites for this course (if any): MTH444
5. Co-requisites for this course (if any)**: N/A**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	22	70 %
2	**Blended**	8	20 %
3	**E-learning**	3	10 %
4	**Correspondence**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	25
2	**Laboratory/Studio**	0
3	**Tutorial**	15
4	**Others** (specify) Seminars and presentations	15
	Total	

B. Course Objectives and Learning Outcomes

1. Course Description

On successful completion of the module, students should be able to:

- Know the importance of the coding theory
- How he can make some elementary codes
- Know all the tools used in linear codes
- Extract the generator of a code
- Construct the dual code of a given linear code
- Correct some errors induced by the canal
- Determine the Hamming distance between two words code

2. Course Main Objective

The course is self-contained and doesn't need to be changed. However, the computer can be used intensively to make the course sufficiently clear and this needs to install many software as Mathematica, Macauley, Matlab and other…

3. Course Learning Outcomes

CLOs		Aligned-PLOs
1	**Knowledge and Understanding**	
1.1	We give an overview on the history of the cryptography and introduce the symmetric cryptography.	We first introduce new notions, , we establish the attached properties, we give and prove different theorems related to those notions. Finally, we construct new examples and concepts. To well fix the principal facts, homework is proposed.
1.2	We introduce The RSA coding and the notion of code correcting.	
1.3	We introduce linear codes, the Hamming codes, dual codes, generating Matrix and many notions related to linear codes .	
1.4	We study the mathematical ideas underlying modern coding theory and cryptography, including algebra, number theory and probability theory..	
1.5	We present the basic theory and objectives of each of these steps, together with the basics of information theory.	
2	**Skills :**	
2.1	The ability to extract the generator of a code.	
2.2	The ability to Construct the dual code of a given linear code	
3	**Values:**	
3.1		
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Account	6h
2	Study the Z / nZ ring	3h
3	History of cryptography	3h
4	Modern symmetric encryption	3h
5	Additional topics in account theory	3h

6	RSA encryption.	3h
7	Introduction to Corrected Encryption	3h
8	Homing and linear cipher binary spaces	6h
9	Binary code and linear code	3h
10	Linear code applications	6h
11	The linear code and protection of information and data	3h
Total		42

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	Study the arithmetic on $\mathbb{Z}$, the ring $\mathbb{Z}$ / $n\mathbb{Z}$ and then the field $\mathbb{Z}$ / $p\mathbb{Z}$..	We first introduce new notions, give examples from the simple ones (numbers sets) to those related to cryptography. we establish the attached properties, we give and prove different theorems related to those notions.	-MCQ on principal theorems -Proving additional notions that can been elaborated from the general study -In general we introduce a short question to control the ability of the student to make the relationship between all the parts of the course.
1.2	Give an overview on the history of the cryptography and introduce the symmetric cryptography.		
1.3	Introduce The RSA coding and the notion of code correcting.		
1.4	Introduce and study linear codes, the Hamming codes, dual codes, generating		
1.5	Introduce and study modern coding theory and cryptography, including algebra, number theory and probability theory.		
1.6	Address the efficient error free and secure delivery of information using binary data streams.		
1.7	Construct new finite fields in view to be applied to coding and cryptography.		
1.8	Employ channel coding to minimize the effects of errors.		
2.0	**Skills**		
2.1	The ability to extract the generator of a code.	Explanations and examples given in lectures.	Short questions and discussion during the tutorial class+ short quizzes.
2.2	The ability to Construct the dual code of a given linear code.	Guidance and supervision of the work developed in tutorial classes.	
2.3	To have the ability to make different codes.	By using many examples	
2.4	To have the ability to encrypt and decrypt texts.		
3.0	**Values**		

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
3.1	The students should be able to formulate and solve mathematical problems such as:	**Direct teaching**: Lectures **Aimed teaching**: Discovery and oral questions **Indirect teaching**: Cooperative Learning	• Homework • Quiz • Midterms • Final Exams
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	**1**	**Midterm 1**	**7th week**
2	**3**	**Homework**	**Through of semester**
3	**4**	**Quizzes**	**Through of semester**
4	**5**	**Electronic Test**	**13th week**
5	**6**	**Presentation**	**Through of semester**
6	**7**	**Final exam**	**End of semester**
7	**1**	**Midterm 1**	**7th week**
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:

1- 3-office hours per week in the lecturer schedule.

2- The contact with students by e-mail and website.

3- activation of the virtual classrooms and academic guidance via Black Board **LMS**.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	- An Introduction to information communication and cryptography- Norman L.Biggs-Springer Undergraduate Mathematics Series 2008 - Introduction to Cryptography with Coding Theory-Trappe-Pearson-Lawrence C. Washington Wide.
Essential References Materials	Cryptography: Theory and practice –Doug Stinson- Originally published-Editor Doug Stinson-1995.
Electronic Materials	http://www.gap-system.org/Releases/index.html
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	- Classroom with capacity of 30-students. - Computer Lab of Mathematics Department
Technology Resources (AV, data show, Smart Board, software, etc.)	Mathematical software packages like MATHEMATICA
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	https://www.intmath.com/plane-analytic-geometry/intro.php http://mathworld.wolfram.com/topics/Geometry.html

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students/ internal committee	Direct (Students evaluation electronically organized by Deanship of registration and admission)/ Verification of students' papers
Extent of achievement of course learning outcomes	Staff members (Peer Reviewer)	Indirect (Frequent meetings consultation among the teaching staffs)
Quality of learning resources.	Staff members (course coordinators)	Direct (Meeting between course coordinators and the tutors)

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	Mathematics Department
Reference No.	27
Date	8/8/1442 H -21/3/2021 G

Head of Department

Dr. Muqrin Almuqrin