هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

2023
TP-153

Course Specification
(Bachelor)

Course Title:	**Applications of Algebra**
Course Code:	**2024110-3**
Program:	Bachelor in Mathematics
Department:	Mathematics and Statistics Department
College:	**Faculty of Sciences**
Institution:	**Taif University**
Version:	1
Last Revision Date:	20/05/2023

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: 3(3,0,0)

2. Course type

A.	☐University	☐College	☒ Department	☐ Track	☐Others
B.	☐ Required		☒ Elective		

3. Level/year at which this course is offered: Level 7 / Fourth Year

4. Course general Description:

This course introduces the students to cryptography and coding theory as applications of abstract algebra through presenting some simple cryptosystems, some techniques of cryptanalysis and linear codes, group codes.

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

Ring Theory (2023203-3)

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

None

7. Course Main Objective(s):

The student will be taught as follows:

- **Introducing interesting and useful applications of abstract algebra.**
- **Training the students to use knowledge of mathematics in coding theory and cryptography.**
- **Learning the most modern applications.**

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	**3Hr /Week**	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		

No	Mode of Instruction	Contact Hours	Percentage
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
2.	**Laboratory/Studio**	NA
3.	**Field**	NA
4.	**Tutorial**	NA
5.	**Others (specify)**	NA
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	Recognize fundamentals of ring theory and group theory professionally in cryptography and coding theory.	K1	• Interactive classes • Self-learning through the website • A rich variety of mathematical tasks and projects `	• Exams • Assignments
1.2	Outline some “Simple Cryptosystems” Error-Detecting, Correcting Codes.	K1	• Interactive classes • Self-learning through the website • A rich variety of mathematical tasks and projects	• Exams • Assignments
1.3	Describe the type of Group codes.	K1	• Interactive classes • Self-learning through the website • A rich variety of mathematical tasks and projects	• Exams • Assignments

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
2.0	**Skills**			
2.1	Apply appropriate properties of ring theory and group theory to prove some principles, theorems, formulas on cryptography and coding theory.	S2	• Interactive classes • Self-learning through applying properties on more complicated problems on cryptography and coding theory • Group discussions	• Quizzes • Assignments
2.2	Explain the type of a given “Cipher”.	S2	• Interactive classes • Self-learning through applying properties on more complicated problems on cryptography and coding theory • Group discussions	• Exams • Quizzes
3.0	**Values, autonomy, and responsibility**			
3.1	Work effectively within groups and independently.	V1	• Projects	Oral presentation of the projects

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to Cryptography (Private Key Cryptography- Public Key Cryptography),	3
2.	Classical Cryptography- Some simple Cryptosystems: Shift Cipher	3
3.	Substitution Cipher- Affine Cipher	3
4.	Permutation Cipher- Hill Cipher	3
5.	Stream Cipher (Auto-Key Cipher)	3
6.,7.	Linear Recursive Cipher	6
8.	**First Midterm exam**	3
9.	Cryptanalysis: Cryptanalysis of the Substitution Cipher	3
10.	Cryptanalysis of the Linear feedback shift register Stream Cipher	3
11.	Algebraic Coding (Error Detecting)	3
12	Correcting Codes	3
13.	**Second Midterm exam**	3
14.,15.	Linear Codes, Group Codes (Coset Decoding)	6
Total		45

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	Continuous Evaluation	10 %
2.	Assignments, report	Continuous Evaluation	10 %
3.	Midterm 1 Exam	8-9	15%
4.	Midterm 2 Exam	12-13	15%
5.	Final Exam	15-16	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	D. R. Stinson, Cryptography, Theory and Practice, 4th Edition, Chapman & Hall, 2018.
Supportive References	J. A. Buchmann, Introduction to Cryptography, 1st Edition, Springer, 2001.
Electronic Materials	Lectures available in Blackboard
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms
Technology equipment (Projector, smart board, software)	Data show, Blackboard
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, Program Leader	Direct & Indirect
Effectiveness of students assessment	Faculty, Program Leader	Direct
Quality of learning resources	Students, Faculty	Indirect

Assessment Areas/Issues	Assessor	Assessment Methods
The extent to which CLOs have been achieved	Faculty	Direct & Indirect
Other		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	Department Council
REFERENCE NO.	4
DATE	October 2023

قسم الرياضيات والإحصاء
Mathematics and Statistics Department
TU
جامعة الطائف
TAIF UNIVERSITY