Course Specification
(Bachelor)

Course Title:	**Introduction to Cryptography and Coding**
Course Code:	**MAT 1361**
Program:	**Bachelor of Science in Applied Mathematics**
Department:	**Mathematics and Statistics**
College:	**Science**
Institution:	**Imam Mohammad Ibn Saud Islamic University**
Version:	**2024 – V1**
Last Revision Date:	**08/10/2024**

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours:					
3 (2 Lectures, 0 Lab, 2 Tutorial)					
2. Course type					
A.	☐University	☐ College	☒ Program	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: Level 6 / Year 3					
4. Course general Description:					
The course offers a comprehensive introduction to both classical and modern cryptographic techniques and coding theory. Students will explore classical ciphers like the Vigenère and Hill ciphers, delve into public-key cryptosystems including RSA and ElGamal, and learn about digital signatures for ensuring authenticity. The course also covers foundational concepts in coding theory, such as error detection and correction, linear codes, and cyclic codes.					
5. Pre-requirements for this course (if any):					
MAT 1321 Modern Algebra					
6. Co-requisites for this course (if any):					
None.					
7. Course Main Objective(s):					
The course is essential in the BSc in Applied Mathematics program as it integrates theoretical mathematics with practical applications in security and data protection. It develops students' analytical and problem-solving skills through the study of cryptographic algorithms and coding techniques, preparing them for careers in cybersecurity and data analysis while promoting interdisciplinary knowledge in mathematics and computer science.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%
2	E-learning	0	0%
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**	30

2.	**Laboratory/Studio**	0
3.	**Field**	0
4.	**Tutorial**	30
5.	**Others (specify)**	0
Total		60

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	To outline the principles of cryptology and of cryptanalysis of historical ciphers.	K1, K2	2 lecture hours\week	Regular Exams
1.2	To recognize the theory and practice of coding and modern cryptographic systems.	K1, K2	2 tutorial hours\week Self-study	Assignments Short Quizzes
2.0	**Skills**			
2.1	To develop basic techniques of coding.	S1, S2	Real-life problems	Short Quizzes
2.2	To present main algorithms in public key cryptography clearly and precisely both orally and in writing.	S4	Self-study	Participations
2.3	To use Internet in searching for up-to-date algorithms in cryptography.	S5	Real-life problems	Short Quizzes
2.4	To demonstrate the validity of some cryptography algorithms.	S3	Self-study	Participations
3.0	**Values, autonomy, and responsibility**			
3.1	To engage in group discussions and critical interactions	V1, V3	Personal questions	Participation
3.2	To differentiate between valid and fallacious Mathematical arguments to model real problem involving differential equations.	V1, V2	Teamwork	Homework and Mini-projects

C. Course Content

No	List of Topics	Contact Hours
1.	**Classical Cryptography:** Introduction, shift ciphers and substitution ciphers, Affine cipher, Vigenere cipher, Permutation cipher, Hill cipher, stream cipher, Introduction to cryptanalysis, cryptanalysis of classical systems.	**20**
2.	**Public-key cryptosystems:** RSA, Number Theory facts, Discrete logarithm, ElGamal cryptosystem, Massey-Omura cryptosystem, Diffie-Hellman key agreement.	**10**
3.	**Digital signatures:** RSA signature, El-Gamal signature, Digital signature algorithm.	**10**
4.	**Introduction to Coding Theory:** Introduction to codes, Hamming distance, error detection, error correction, information rate. Linear codes, Generator matrix and parity-check matrix, Perfect codes.	**15**
5.	**Cyclic codes:** Cyclic codes, generator polynomials.	**5**
Total		**60**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	HomeWorks, Quizzes, Mini-projects	During the term	10%
2.	First Midterm	Week 5-6	25%
3.	Second Midterm	Week 10-11	25%
4.	Final Exam	Week 15	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	• *Cryptography: Theory and practice,* **Douglas R. Stinson, 3rd Edition, 2006, Chapman and Hall/CRC. (Main Reference).** • *Coding Theory: A First course, San Ling, Chaoping Xing, Cambridge University Press, 2004*

Supportive References	• *Introduction to Modern Cryptography,* **J. Katz, Y. Lindell, Chapman and Hall/CRC, 1st Edition, 2007.** • *Making, Breaking Codes: An Introduction to Cryptology,* **Paul Garrett, 2001, Prentice-Hall.** • *A First Course in Coding Theory, R. Hill, Oxford University Press, 1997.*
Electronic Materials	
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• **Classrooms:** Equipped with whiteboards, projectors, and Smart Boards for interactive lessons and group discussions. • **Laboratories:** Feature computers with internet access, enabling hands-on activities and exploration of algebraic and trigonometric concepts. • **Exhibition Rooms:** Spaces for showcasing projects and presentations to encourage collaborative learning.
Technology equipment (projector, smart board, software)	• **Data Show Projectors:** For clear presentations in classrooms and labs. • **Smart Boards:** To enhance interactivity during lessons. • **Mathematical Software:** Essential for graphing and analysis.
Other equipment (depending on the nature of the specialty)	• **Computers:** For mini-project and homework and practical applications in laboratories. • **Advanced Calculators:** For computations and problem-solving and supporting the study of limits, continuity, and differentiation. • **Whiteboards and Markers:** To facilitate brainstorming and collaboration.

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Student and teaching staff	Surveys and Questionnaires
Effectiveness of Students assessment	Course Coordinator	Peer Reviews
Quality of learning resources	Students and teaching staff	Classroom Observations
The extent to which CLOs have been achieved	Student Representatives	Student Performance Evaluations (exams, projects) CLOs Excel sheet.
Other	**None**	

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	**MATHEMATICS AND STATISTICS DEPARTMENT COUNCIL**
REFERENCE NO.	**8/1446**

DATE	**05/04/1446 (08/10/2024)**