SYLLABUS

Course Code	*Course Num.*	*Course Name*	*Credit Hours*	*Lec.*	*Lab.*	*Tut.*	*Private study*	*Pre-requisites*	*Course Level*	*Teaching Language*
MAT	**661**	**Coding Theory & Cryptography**	**4**	**3**	**٠**	**1**	**9**	**MAT 623**	**2^1-2^2**	**English**

A. Course Description

This course describes the most important ideas and theoretical results in linear codes and their construction. It also introduces to cryptography.

B. Course Outcomes

At the end of this course the student will be able to*:*

Know the basic topics in Coding Theory and Cryptography: Linear Codes and their constructions, Public key cryptosystems, Hash Functions and Signature Schemes, the cryptographic standards DES and AES

C. References:

1. **D. Hankerson & others,** *Coding Theory and Cryptography: The Essentials*; Marcel Dekker, 2nd Ed., 2000. (Main Reference)

Required Textbook

2. **S. Ling, C. Xing,** *Coding Theory: A First Course*; Cambridge University Press, 1st ed. 2004.
3. **J. van Lint,** *Introduction to Coding Theory*; Springer 3rd Ed. 1998.
4. **S. Lin, D. Castello,** *Error Correcting Codes*; Prentice Hal, 2nd ed. 2004.

Course Website: Google Classroom Webpage:http://www.imamm.org/

D. Topics Outline

1. **Basics and Linear Codes:** Error detection, correction and decoding, Hamming distance and distance of a code, MLD reliability, Linear codes and their basis, Generator matrix and parity-check matrix, Equivalence of linear codes, Encoding with linear codes, Cosets of linear codes and the coset leader, Nearest neighbor decoding.
2. **Bounds and Constructions of Linear Codes**: Optimal codes, extended codes and parity-check matrices, Bounds for codes and their types, Perfect codes, Hamming codes and their use, Golay codes, Reed-Muller codes and their use.
3. **Cyclic Codes and Other Codes:** Cyclic Hamming codes, BCH codes and their use, Codes over $GF(2^n)$, Reed-Solomon codes, Quadratic-residue codes, Hadamard matrix codes, Nordstrom-Robinson code, Preparata codes and Kerdock codes, Propagation rules of constructing linear codes, First order and higher Reed-Muller codes, Subfield codes.
4. **Classic Cryptography:** Encryption Schemes, Symmetric key encryption, Fiestel Cipher and DES.
5. **Public-Key Cryptography** (PKC): Algorithm and Complexity, Quadratic residues and quadratic reciprocity, Primality testing, Discrete algorithm, Hash functions, RSA, Provable security and ELGamal, Cryptography protocols (Diffe Hellman, Zero Knowledge and coin-tossing).

E. Office Hours

Office hours give students the opportunity to ask in-depth questions and to explore points of confusion or interest that cannot be fully addressed in class.

F. Exams & Grading System

The semi-official dates of the exams for this course are:

- **Midterm :** 8th or 9th week.
- **Quizzes & Homeworks:** During the semester.
- **Final Exam:** 16th week.

Your course grade will be based on your semester work as follows:

Midterm : 30 %	**Final Exam:** 40 %
Quizzes, Homework, Attendance & Participation: 30 %	

The grading distribution:

A^+	A	B^+	B	C^+	C	F
[95, 100]	[90, 95)	[85, 90)	[80, 85)	[75, 80)	[70, 75)	[0, 70)

G. Student Attendance/Absence

Only three situations will be considered as possible excused absences:

- Occurrence of a birth or death in the immediate family will be excused. (“Immediate family” is defined by the University as spouse, grandparents, parents, brother, or sister).
- Severe illness in which a student is under the care of a doctor and physically unable to attend class will be excused. Students are not excused for a doctor's appointment. Do not make appointments that conflict with rehearsals. Notes from the University Health Center will be accepted.

Executive Rules for Study Regulations and Examsgoo.gl/ykm7t3