SYLLABUS

Course Code	*Course Num.*	*Course Name*	*Credit Hours*	*Lec.*	*Lab.*	*Tut.*	*Private study*	*Pre-requisites*	*Course Level*	*Teaching Language*
MAT	**461**	**Introduction to Cryptography and Coding**	**4**	**3**	**0**	**2**	**6**	**MAT 321**	**7[1]**	**English**

A. Course Description

The course is devoted to the fields of cryptography and coding theory. It gives an introduction, with proofs, to the algebra and number theory used in coding and cryptography. Basic problems of cryptography and coding are discussed. Topics include classical ciphers, public key cryptosystems (RSA, Diffie-Hellman key exchange, ElGamal), digital signatures, codes, linear codes, perfect codes and cyclic codes.

B. Course Outcomes

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

- Be familiar with Cryptography and Coding theory.
- To use basics of cryptography, public-key systems and digital signatures.
- Be familiar with coding theory, especially cyclic codes.

C. References:

Required Textbook

- *Cryptography: Theory and practice*, Douglas R. Stinson, 3rd Edition, 2006, Chapman and Hall/CRC.
- *Coding Theory: A First course*, San Ling, Chaoping Xing, Cambridge University Press, 2004.

Other 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.

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

[1] *B.Sc. in Applied Mathematics.*

D. Topics Outline

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.
2. **Public-key Cryptosystems:** RSA, Number Theory facts, Discrete logarithm, ElGamal Cryptosystem, Massey-Omura Cryptosystem, Diffie-Hellman Key Agreement.
3. **Digital Signatures:** RSA Signature, El-Gamal Signature, Digital Signature Algorithm.
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.
5. **Cyclic codes:** Cyclic Codes, Generator Polynomials.

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 1:** 6th or 7th week.
- **Midterm 2:** 11th or 12th week.
- **Quizzes & Homeworks:** During the semester.
- **Final Exam:** 16th week.

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

Midterm 1: 20 %	**Midterm 2:** 20 %	**Final Exam:** 40 %
Quizzes, Homework, Attendance & Participation: 20 %		

The grading distribution:

A$^+$	A	B$^+$	B	C$^+$	C	D$^+$	D	F
[95, 100]	[90, 95)	[85, 90)	[80, 85)	[75, 80)	[70, 75)	[65, 70)	[60, 65)	[0, 60)

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 Exams
goo.gl/ykm7t3