Name of the University: Middle East Technical University

Name of the Department: Institute of Applied Mathematics – Cryptography Program

Course Code: IAM 511

Full Name of the Course: Algorithms and Complexity

Section of the Course: 01

Academic Year / Semester: 2015-16/1

Instructor Information

Name/Title: Murat Cenk

Office Address: Institute of Applied Mathematics -228

E-Mail Address: mcenk@metu.edu.tr

Personal Website: -

Office Phone: 210 5689

Mailbox Location: Institute of Applied Mathematics

Office Hours: 

Course Assistants Information (if any): Ahmet Sinak (ahmet.sinak@metu.edu.tr)

Course Information

Prerequisites: Consent of the instructor

Credit / ECTS: (3-0)3 / 8.0

Class Days:

Class Hours:

Location of the Class: IAM

Lab/Studio Hours & Location (if any): N/A

Course Catalogue Description: Formal techniques for design and analysis of algorithms, methods for specifying algorithms, proving an algorithm’s correctness, basics of algorithmic efficiency, asymptotic notations and basic efficiency classes, computational complexity, complexity classes P, NP, NP-completeness/hardness, mathematical analysis of algorithms, divide-and-conquer, space and time trade-offs, and number-theoretical algorithms.

Course Objectives: The aim of the course is to present the basic topics in algorithms and complexity needed in cryptography. The fundamental algorithms in cryptography will be introduced and their complexities will be studied.

Course Learning Outcomes: Students are going to be familiar with the design and analysis of algorithms used in cryptography. They will be able to compute the complexities of the algorithms and to design new algorithms with the improved complexities.
Program Outcomes Matrix/Table: -

ECTS Workload Table: -

Instructional Methods: Classical lecture

Course Website/Course Management System:

Weekly Outline/Tentative Course Schedule:

WEEKS: 1-2:
- Fundamentals of algorithm problem solving
- Important problem types: Sorting, searching, graph
- Fundamental data structures.

WEEKS: 3-6:
- Analysis of algorithm efficiency
- Time estimate for doing arithmetic: Big-O Notation
- Number-theoretical algorithms and their complexity: Euclidean algorithm, Repeated Squaring Algorithm, Chinese remainder theorem, Multiplication Algorithm and Quadratic Residues

WEEKS: 7-8
- Complexity theory in cryptography
- Randomized algorithms and complexity classes P, NP, NP-completeness/hardness
- Reducing one problem to another

WEEKS: 9-11:
Design and analysis techniques:
- Brute force and exhaustive search
- Divide-and-conquer
- Space and time trade-offs
- Greedy technique
- Dynamic programming

WEEKS: 12-14:
- Selected algorithms and their complexity analysis: Multiplication of large integers and matrices, FFT computations
- Arithmetic circuits
- Parallel computation

Required Textbook/s & Readings:
• Anany Levitin, Introduction to the design and analysis of algorithms, Pearson, 2012

Required Course Materials (if any): N/A

Course Evaluation: Formal examinations, homework assignments

Information about Exams. Exams will cover the topics covered in the class.

Information about Assignments:

Information about Term Projects (if any): N/A

Information about Field Trips (if any): N/A

Information about other evaluation methods (if any): N/A

Course Grading:
• Homework and project assignments 30%
• 1 Midterm 30%
• 1 Final 40%

Course Policies: N/A

Class Attendance and Participation: N/A

Resit Exams: N/A

Missed Exams/Assignments: There will be no make up examinations for this class and late homework assignments will not be accepted. An exception is when there is an official medical or family emergency, in this case you should contact the instructor as soon as possible.

Late Submission of Assignments: Late submissions are not accepted

Safety Procedures (if any): N/A

Classroom Rules (Eating-Drinking, Use of Mobile Phones and Electronic Devices, Civility…etc.): N/A


Academic Honesty/Integrity/Ethics: All homework, midterms are expected to be individual work. If you use a source (online or offline), you are expected to cite it. Violation of these general principles will be handled based on the university regulations and may result in disciplinary action.

Additional Support Services (Library, Computer Center, L&SD…): N/A
Appendices

Project/Presentation Assessment Rubric: N/A

Peer Assessment/Self-Evaluation Form: N/A

Tips for Success in the Course: N/A