
Lamar University

COSC 5340-01, Fall 2004

Cryptography

Instructor: Dr. Chung-Chih Li
Office: 69 Maes, tel: (409) 880-8748
URL: <http://hal.lamar.edu/~licc>
E-mail: licc@hal.lamar.edu

Office Hours: MWF 10:00 ~ 11:00 AM or by appointment

Class meeting times and place:

MWF 11:15 ~ 12:05 AM, Maes 113
(Attendance will be taken impulsively)

HomePages of the course: http://hal.lamar.edu/~licc/cosc5340_cryp

From there, you can find some important information assignments, assignment data, due dates, sample programs, announcements.

Note: An announcement made in the class **will be considered as an OFFICIAL one**, since I may not be able to update every announcement.

Course Description and Purposes:

In this course we will survey some contemporary cryptographic methods and the theory behind those methods. We start with an introduction to the basic structure and definition of a cryptosystem and some intuitive ways of encryption. These intuitive encryption methods are either vulnerable to cryptanalysis attacks or simply too expensive for parties to communicate. Then, we will move into several protocols that are widely used in contemporary cryptosystems such as DES, AES, RSA, ElGamal, Elliptic Curve.

Since the greatest fun here is to understand the theory behind those modern cryptosystems and number theory is the key foundation that builds up the entire enterprise, we will spend a great deal of time on the subject before we move into any subtle cryptosystem. Besides number theory, the subject in fact intimately relates to many other disciplines such as algorithm analysis, theoretical complexity theory, and machine learning. We will also scratch these touches in the class. Nevertheless, this is not a pure theoretical course, students will be asked to implement several cryptographic algorithms, analyze them, point out the weakness, attack peer student's cryptosystem or some ciphertexts given by the instructor as programming assignment.

Prerequisites: Data Structures, Algorithm Analysis, Discrete Math, Mature C++ programming skill.

Textbooks:

Introduction to Cryptography with Coding Theory, by Wade Trappe & Lawrence C. Washington, Prentice Hall, 2002

Reference:

1. Cryptography: Theory and Practice, Douglas Stinson, Chapman & Hall; 2 edition, 2002

2. Introduction to Cryptography, by Hans Delfs and Helmut Knebl, Springer-Verlag, 2002
3. Introduction to Algorithms, Thomas H. Cormen and Charles E. Leiserson and Ronald L. Rivest, The MIT Press, 1989

Examinations and Dates: (300 points)

All tests are accumulative and open textbooks; but **no notes, no extra paper, no calculators, no computers**. No material can be circulated during the test, including pencil and eraser.

No makeup-test will be given.

A documented absence authorized by the university and approved by the student's academic advisor **may be** used to have *one* missed test dismissed from the final grade.

Midterm I	100 points	(6th week)
Midterm II	100 points	(11th week)
Final Exam	100 points	(16th week, TBA)

Programming Assignments: (250 ~ 300 points)

About 7 or 8 programming assignments will be given. The weight of each program depends on its difficulty. Students are encouraged to discuss assignments and help each other. However, this does not mean that you can either entirely or partially copy or modify someone else's works.

Any form and any degree of plagiarism will receive 0 point.

Late works will be graded with penalty: -10 points per day after the due date.

Attendance: (50 points)

Each attendance, if taken, contributes 5 points towards students' final scores. In other words, an absence on the day the roll is checked costs 5 points.

Pop quizzes: (50 points)

About five pop quizzes will be given impulsively. Each quiz carries 10 points towards students' final scores. The coverage of every quiz is also accumulative, including the materials covered in the class right before the quiz. A typical quiz takes about 10 minutes. On the day a quiz is given, the attendance will not be taken. No makeup quiz will be given if missed. If you miss a quiz due to a university authorized absence, we will use the average of your rest quizzes; otherwise, you get a 0 for the absent quiz.

Grading Policy: At least 650 points will be given. The grade is based on the following scheme.

Points	Grade	
540 ~ 600	A	Excellent
420 ~ 539	B	Good
300 ~ 419	C	Satisfactory
200 ~ 299	D	Passing
0 ~ 199	F	Failure

Curve would not be considered.