

LOYOLA COLLEGE IN MARYLAND



MA 106: Ciphers and Codes Fall 2003

Instructor	Dr. Anne Young, Professor of Mathematical Sciences
Office:	JH 120
e-mail address:	ayoung@loyola.edu
Secretary:	Ms. Ann Burke
Phone:	410-617-2400 (M - F, 8:30 AM - 5 PM)
voice-mail:	To reach Dr. Young's personal voice mailbox, enter 968642 (younga).
Dr Young's Homepage:	www.loyola.edu/academics/academicaffairs/ayoung
Blackboard Login Page:	bb6beta.loyola.edu
Office Hours:	posted weekly on Blackboard and by appointment
Primary Text:	<i>Mathematical Ciphers</i> , Young
Secondary Text:	<i>The Code Book</i> , Simon Singh

Catalogue Course Description: The mathematical basis of elementary ciphers and codes including substitution ciphers, public key ciphers, and RSA system. Topics include elementary number theory and modular arithmetic.

Informal Course Description: The message DOO DUH ZHOFRPH is an example of a cipher. There are many different schemes for creating ciphers; in fact, one of the earliest known methods was used by Julius Caesar. The course will focus on those schemes that have a mathematical basis. It will begin with Caesar's method and end with a scheme currently used for security on the Internet. The mathematics used will be elementary and will be developed in the course.

Chapter 1 in the text contains more information about the content and structure of the course as well as advice from the instructor and former students.

Course Objectives: At the completion of the course, the student will be able to

- explain the difference between cryptography and cryptanalysis
- perform elementary modular arithmetic calculations
- encipher and decipher messages using the Caesar, Multiplication, and Multiplication-Shift Ciphers
- do cryptanalysis for the Caesar, Multiplication, and Multiplication-Shift Ciphers
- find inverses in modular arithmetic using the Euclidean Algorithm method
- encipher and decipher messages using the General Multiplication-Shift and Exponential Ciphers
- explain the difference between private key and public key ciphers
- explain the structure, signature scheme, and security of the RSA Cipher
- explain the difference between substitution and block ciphers
- encipher and decipher messages using the XOR and SDE (Simple DES) Ciphers
- read, summarize, and discuss articles related to cryptography and security issues

Tests: Monday, Sep 29; Wednesday, Oct 29; Friday, Nov 21
Each test will have an in-class part and a take-home part. The dates of the in-class parts are listed above. The take-home part will be distributed at the end of the in-class part and will be due at the start of the next class period.

Final Exam: Friday, Dec 12, 9 - 11 AM

Grading Scale:

$93.0 \leq \text{average}$	A	$77.0 \leq \text{average} < 80.0$	C+
$90.0 \leq \text{average} < 93.0$	A-	$73.0 \leq \text{average} < 77.0$	C
$87.0 \leq \text{average} < 90.0$	B+	$70.0 \leq \text{average} < 73.0$	C-
$83.0 \leq \text{average} < 87.0$	B	$67.0 \leq \text{average} < 70.0$	D+
$80.0 \leq \text{average} < 83.0$	B-	$60.0 \leq \text{average} < 67.0$	D
		$\text{average} < 60.0$	F

Grading: Your grade for this course will be computed as follows:

Exercises	15%
Tasks	5%
Cryptography Project	15%
3 Tests (15% each)	45%
Final Exam	20%

Texts: The primary text is *Mathematical Ciphers*. Unlike some math books you may have used, this one is written for students. You are expected to read and understand every single word. Complete understanding will not necessarily occur on the first or even second reading. Often it will require working through an example on your own and/or asking questions in class. The text is printed in a large font on only one side of the page; you are encouraged to write in the text itself as you read/work through it.

The Code Book is a secondary text. Reading assignments will be given throughout the semester. The book will be the basis for both parts of the Cryptography Project.

Exercises: There will be frequent out-of-class exercises. Late exercises will be assessed a penalty and will not be accepted after the assignment has been discussed in class.

Exercise sheets will be distributed in class. If you misplace a sheet or are absent from class, you will find a copy in the Exercises Section of Blackboard.

Tasks: Tasks are straightforward, time-sensitive assignments. A typical task will involve creating a message for a classmate. If that task is not carried out correctly, by the deadline, your classmate will not be able to complete the next assignment.

Each task will be worth 2 points. Submissions which are slightly late or not completely perfect will earn only 1 point. Late and/or incorrect submissions will receive no credit.

Tasks will be posted in the Announcements Section of Blackboard.

Cryptography Project: Just prior to mid-semester and again at the end of the course, I will ask you to read and summarize material that pertains to cryptography. This material will include selected chapters in *The Code Book* as well as articles posted on the Internet. The first part of the project will be distributed on Wednesday, October 1 and will be due on Wednesday, October 15. The second part will be distributed on Wednesday, November 19 and will be due on Monday, December 8.

Homework: At the end of each class period, an assignment for the next class meeting will be given. This will include textbook reading as well as homework problems. Homework will not be collected or graded. You are encouraged to work with classmates as you resolve questions and master the material.

The assignment for the next class meeting will be posted in the Announcements Section of Blackboard.

Calculator: You will need a calculator. A graphing calculator is highly recommended because of its viewing screen and built-in functions. Be sure to bring your calculator to each and every class.

Blackboard: This class will be part of a pilot group using a new version of Blackboard. The login page (bb6beta.loyola.edu) will not be accessible from Loyola's homepage. You will need to enter the URL or put it in your Favorites list.

Attendance and class participation: Some class time will be devoted to non-lecture activities, including small group work and discussion of homework problems. Consequently, you are expected to be an alert and active participant in each and every class. Of course, it is understood that if you are ill or have an unexpected emergency, you will not be in class. But those should be infrequent occurrences. Attendance will be taken and late arrivals will be noted.

If you do miss a class, you should check the Announcement Section of Blackboard; the assignment, including exercise and/or task, for the next class will be posted there.

Student Athletes: If you are a student athlete, please provide me with your travel and game schedule indicating when you will need to miss class to participate in athletic events. While travel for athletics is an excused absence, you will need to make up any missed work.

Disability Accommodations: To request academic accommodations due to a disability, please contact the Disability Support Services, 4502 A Seton Ct, 410-617-2062, TDD 410-617-2141, or mwiedefeld@loyola.edu. If you have a letter from Disability Support Services indicating that you have a disability that requires academic accommodations, please give it to me so we can discuss the accommodations you might need in this class.

Loyola College Honor Code Statement:

“The Honor Code states that all students of the Loyola Community have been equally entrusted by their peers to conduct themselves honestly on all academic assignments.

The students of this College understand that having collective and individual responsibility for the ethical welfare of their peers exemplifies a commitment to the community. Students who submit materials that are the products of their own minds demonstrate respect for themselves and the community in which they study.

All outside resources or information should be clearly acknowledged. If there is any doubt or question regarding the use and documentation of outside sources for academic assignments, your instructor should be consulted. Any violations of the Honor Code will be handled by the Honor Council.”

The Honor Code as it Pertains to this Class: The Honor Code rules for each Exercise will appear on the assignment sheet. It is your responsibility to ask for clarification if you have any questions about what is or is not permitted. For each assignment, you must sign a statement that you understand and have adhered to the Honor Code as it applies to that work. This statement is required by the Honor Council.