Math 108-01
Cryptology
CRN# 21233
TR 2:00pm to 3:15pm
Rhodes Tower 410

Instructor:	Dr. Christopher Seaton	
Office:	320 Ohlendorf Hall	
Office Hours:	MW: 1:00pm to 2:30pm	
	TR: 10:00am to 10:50am	*or by appointment*
Phone:	x3721	
E-mail:	seatonc@rhodes.edu	
Web:	http://www.faculty.rhodes.edu/seaton/	
Text:	T. Barr: **Invitation to Cryptology**, Prentice Hall, 2002	

Course Description:

The purpose of this course is to examine selected classical and modern methods of message encryption, decryption, and cryptanalysis. In this context, we will develop and use a variety of mathematical tools to describe and study the methods: modular arithmetic, probability, matrix arithmetic, number theory, Boolean functions, and complexity theory.

In governments, military organizations, banks, commercial concerns, industries, and ordinary life, there is often a need to communicate where the medium is insecure. Discussions between an ambassador and his or her home government officials about diplomatic strategies may need to be kept from another government with which the ambassador is carrying on negotiations. Orders about battlefield tactics from a central command to soldiers should not fall into the hands of the enemy. A transmission from an automatic teller machine to the bank's main office containing a patron's account and balance information should not be readable by thieves. An on-line retailer (or a customer) does not want the credit card numbers of people ordering its products to be obtained by thieves. A company transmitting sensitive or proprietary information among its offices in geographically diverse locations does not want its trade secrets to land in the hands of its competitors. Two individuals corresponding by email may not want their communications to be readable by packet sniffers. These are some of the basic and direct application areas for **cryptography,** the science and art of secret writing.

On the other hand, law enforcement may be monitoring encrypted communications among suspected criminals. The military of one country may be gathering transmissions between an enemy state and its allies or between the state and its armed forces in the field in an attempt to read them and improve their own strategic effectiveness. Turning such "scrambled" communications into comprehensible messages is the process of **cryptanalysis,** which can be a difficult undertaking and one that can be aided by mathematical techniques.

To understand the effectiveness of a cryptographic method, a designer or user of the method not only needs to be able to carry through the steps of encryption and decryption accurately and efficiently, but he or she needs to play the role of cryptanalyst on the method. So the activities of cryptography and cryptanalysis are intimately related; together they are often referred to as **cryptology**.

Content

We will at least cover Chapters 1 and 2, Sections 3.1—3, and Sections 4.1—4. Time permitting, we may cover additional sections of Chapters 3 and 4.

Prerequisites

This course assumes minimal background and is appropriate for Rhodes students who have not taken other math courses after high school.

Office Hours:

Students are **strongly** encouraged to take advantage of my office hours and make appointments at other times. My schedule is at http://faculty.rhodes.edu/seaton/schedule.htm. Please consult this schedule before suggesting an appointment time (particularly via e-mail).

Web-Page:

This syllabus is available on my web-page (URL above). I will post a summary of homework assignments there as well. In addition, I will occasionally use files in class which will be made available in my public folder on the Rhodes academic fileserver. I will announce anything I post in class, but students are encouraged to consult my web page and public folder on the fileserver, particularly if they have missed a class.

The homework summary is for your reference when preparing for class or studying for an exam. It is subject to change until the assignments have been given in class.

Attendance Policy:

I will take attendance. You are permitted **two** unexcused absences throughout the semester; if you are absent two or fewer times, you will be allowed to skip one problem on the final for which you will receive full credit (one tenth of the test). An excused absence must be discussed with me **in advance if possible**, and the proper documentation must be made available where appropriate. If I decide that excessive absences are jeopardizing your ability to pass the course, I will take action as outlined on page 71 of the catalogue. It is your responsibility to obtain notes and assignments, including graded homework, when you are absent.

Grading:

Your letter grade for the course will be based on the following scale:

A	[93, 100]	B-	[80, 83)	D+	[67, 70)
A-	[90, 93)	C+	[77, 80)	D	[63, 67)
B+	[87, 90)	C	[73, 77)	D-	[60, 63)
B	[83, 87)	C-	[70, 73)	F	[0, 60)

This scale is "worst case scenario"; I may choose to uniformly reduce the numerical requirements for a grade, but will not increase them.

The total percentage will be computed as follows:

Homework:	25%
Quizzes:	10%
Exams:	2 × 20%
Final Exam:	25%

Homework:

At the end of each lecture, I will assign both practice problems for you to test your comprehension and homework problems to be handed in. Much of what you learn in this course will be the result of working exercises from the text. These are designed to reinforce key concepts, so keeping up with and doing the assignments is essential to success. The amount of time needed to do homework may vary considerably from assignment to assignment and from student to student. It is not unreasonable to spend **two or three hours** on many of these

assignments, so it is incumbent upon you to allocate time in your schedule for the purpose of doing mathematics homework.

The homework from each week is due the following **Thursday** (modifications may be announced in the case of a holiday or exam week). The homework you hand in must be your own work; you may work on the problems with other students, but they **may not aide in the write-up**.

LATE HOMEWORK WILL NOT BE ACCEPTED.

Quizzes:

At the beginning of most lectures, a short quiz will be given on the reading assignment for that lecture. These quizzes will not assume that you have mastered the material, but will test your familiarity with the reading.

Tests:

There will be two tests, which will be given in FJC from 7:00pm to 8:30pm on Thursday, Feb. 17th and Thursday, March 31st.

If you have to be absent for an exam, you **must** make arrangements with me as early as possible **before** the day of the exam, and you will be expected to document your absence. Otherwise, you will not be allowed to make up the test. **In most circumstances, I will not make arrangements for you to make up an exam unless I have been notified one week before the day of the exam.**

Final Exam:

The final exam is scheduled on Friday, May 6th at 8:30am. It will be a closed-book, closed-notes, cumulative exam. An alternate exam time will be offered on Tuesday, May 2nd at 5:30pm; students interested in taking the final at the alternate time must make arrangements with me at one week in advance.

Math Support Center:

The Math Support Center is a resource for students located on the third floor of Ohlendorf. Our tutor this semester is Jake Smith (smijm@rhodes.edu); Jake will hold drop-in hours from **6pm to 7pm on Monday and Wednesday evenings** to assist you with mastering the material. The first day of drop-in hours will be Wednesday, January 19th. I will e-mail you with any changes to this schedule.

Calculators:

I will allow the use of calculators on the exams, including the final. However, you may not use your calculator to store any formulas or notes, nor may you use advanced features such as matrix operations. I will require you to show your work on homework and exams for full credit.

Honor Code:

All students are expected to conduct themselves within the guidelines of the College's Honor Code. Please ask me if you have any questions about what is allowed. I reserve the right to reduce a student's grade in the event of plagiarism whose intent cannot be verified.

Students with Disabilities:

If you have or think you may have a documented disability, please contact me and the Office of Student Disability Services as early in the semester as possible.