Time: TR 2:30-3:45  
Classroom: ALT 213  
Instructor: Dr. Dena Morton  
Office: Hinkle 111  
Phone: x3674  
Office Hours:  
- Mondays from 2:45-4:00  
- Tuesdays from 11-11:30, 12:25-12:55 and 4:00-4:30  
- Thursdays from 12:25-12:55 and 4:00-4:30  
and by appointment  
e-mail: morton@xavier.edu  
  Note: this is the best way to reach me – I check my e-mail on a regular basis.  
Web Page: http://cerebro.xu.edu/~morton/  
  Note: homework is posted daily. If you miss a class, go to the webpage to find the correct homework.  

Texts and Computer Programs:  
1. Introduction to Cryptography with Coding Theory, 2nd Edition by Wade Trappe and Lawrence C. Washington  
2. The Code Book, by Simon Singh  
3. Maple will be used on a regular basis in class, for homework, and for the exams. (If you do not have access to Maple please let me know.)

Purpose and Content: In this course we will be exploring cryptography – the making and breaking of secret ciphers and codes. We will start with classical ciphers: shift, affine, Vigenère, substitution, Hill, one-time pads, Enigma, etc. Then after a brief introduction to number theory, we will start on modern methods: the RSA algorithm, DES, and AES: Rijndael. If time permits, we will also explore discrete logarithms and elliptic curves. All codes will be placed in historical perspective by exploring the political and military contexts in which they were devised, through readings in The Code Book.

It is essential that you be conscientious about completing both the reading and the computation assignments on time, and at least attempt every assigned problem. Questions are welcome at any time during class. I encourage you to participate actively in class by asking questions and by answering questions posed by either myself or by other students.

Class Activities: Classes will consist of small group activities, discussion, individual activities, and lectures.

Homework: Homework will be assigned (sort of) weekly. Doing homework for this course is the best way for you to pinpoint difficulties. It is also a wonderful learning tool. I will take questions about the homework at the beginning of each class session.

Quizzes: Weekly quizzes will be given on most Thursdays. I will grade these on a 5-point scale. The lowest quiz score will be dropped, so makeup quizzes will not be given under any circumstances. Quizzes will not be given during exam weeks.

Exams: There will be two exams given throughout the semester. There will also be a comprehensive final exam. If you must miss an exam for religious or academic reasons, or in cases of illness or emergency, you must submit a written excuse. A makeup may be scheduled -- this will be decided on a case-by-case basis.

Grading:  
- Weekly quiz performance: 6%  
- Two exams: 18% each  
- Weekly graded problem sets: 30%  
- Research paper: 8%  
- Final exam (cumulative): 20%
Each exam, quiz, etc. will be curved separately and assigned a number grade between 0.0 (the lowest possible F) and 5.0 (the highest possible A). I will announce the cutoffs when returning the exam. If, for example, the cutoff for an A is 87 and the cutoff for a B is 71 and you get an 83, then the number grade corresponding to your 83 would be a 3.75 (B corresponds to 3.0 and you are 12/16=.75 of the way to the next cutoff). The homework and quizzes will be treated similarly. The total course grade may be curved further (that is, a 3.9 would result in an A or A- in the course), but the resulting curve will never lower your grade (that is, a 4.1 would always result in at least an A- in the course). +/- grades may be assigned in borderline cases. I reserve the right to assign a grade of “F” to any student who earns less than 50% on the final exam.

**Important Dates:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday, Jan 16</td>
<td>MLK, Jr. day (no classes)</td>
</tr>
<tr>
<td>Tuesday, Feb. 21</td>
<td>Exam I (tentatively scheduled)</td>
</tr>
<tr>
<td>Monday, Feb. 27-</td>
<td>Spring Holiday (no classes)</td>
</tr>
<tr>
<td>Friday, March 3</td>
<td>Last day to withdraw</td>
</tr>
<tr>
<td>Monday, Apr. 10</td>
<td>Last day to withdraw</td>
</tr>
<tr>
<td>Thursday, Apr. 13-</td>
<td>Easter Holiday (no classes)</td>
</tr>
<tr>
<td>Monday, Apr. 17</td>
<td></td>
</tr>
<tr>
<td>Thursday, Apr. 20</td>
<td>Exam II (very tentatively scheduled – may be earlier)</td>
</tr>
<tr>
<td>Friday, Apr. 28</td>
<td></td>
</tr>
<tr>
<td>Monday, May 2 or</td>
<td>Final Exam (Exact date TBA later)</td>
</tr>
<tr>
<td>Thursday, May 5</td>
<td></td>
</tr>
</tbody>
</table>

**Attendance:** Class attendance is crucial. Lectures include the introduction and explanation of new topics, explorations of graphing calculators, and solutions of calculus problems. Class notes are to be used in conjunction with the text, in order to elicit a fuller understanding of Calculus.

*Please be courteous and come to class on time!*  
*Please turn off your cell phones!*

University policies on attendance are stated on p.47 of the undergraduate catalog.

**Group Work:** Working in a group can be beneficial for everyone involved, provided that you do not abuse the privilege. Make sure that everyone in your group is making a contribution. Do not copy answers from one another, as this will only backfire against you come test-time. Instead, let concepts gel after group discussion, and then write up the solutions by yourself.

**Academic Honesty:** You are expected to conduct yourself with integrity in this course. Cheating will be dealt with as harshly as University regulations permit; measures will be taken during exams to prevent cheating. Students are directed to p. 52 of the undergraduate bulletin for further information.

**How to Do Well in this Course:** Come to class! Read the texts! Come visit me during office hours! Try the problems! Smile! Study hard! Read your class notes! Make sure you keep up with the material in class! Review your class notes! Don’t Panic! Enjoy! Most important of all, if you feel that you are falling behind, or that you do not understand a certain topic, or if you would just like to discuss a mathematical idea (or anything else), come to visit me in my office. That’s why I am here!