MAT 198 : Secrets, Codes, and Ciphers (FY, QR)
TF: 12:30-1:45 in WH 231
Credits: 3 Credits
General Education: FY and QR
Prerequisite: General Education Math Placement

Dr. Charles Rocca
White Hall 322-A
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

Office Hours:

- MTRF: 11:00 am to 12:00 pm
- M: 2:00 pm to 3:00 pm
- or by appointment

Course Materials:

- Text: *The Code Book*, by Simon Singh ($13 paperback on Amazon.com)
- Other Supplies: At least a basic scientific calculator and note cards (3" by 5") for making flash-cards

Course Description:

The fates of nations have been decided by their ability to keep their own secrets while discovering those of their enemies. While Caesar triumphed, Mary Queen of Scots and Hitler fell. Cryptology, the science of secrets, has been dabbled in by amateurs, experts, and presidents. Some of the most successful code breakers were even accused of witchcraft. We will explore their stories and examine the roll played by math in their successes and failures. Prerequisite: General Education Math Placement, General Education: FY and QR.

Content Outcomes:

After successful completion of this course a student will be able to demonstrate …

1. understanding of the how codes and ciphers have effected history.
2. knowledge of the contributions of mathematics to secrecy.
3. how to analyze data an enciphered message in order to glean information about the message.
4. that they have learned to break ciphers and read messages based on limited information.

Through these outcomes students will show that they can *analyze, apply, interpret,* and *represent* quantitative (and qualitative) information in a constructive manner and thus satisfy the Quantitative Reasoning (QR) general education competency.

First Year Outcomes:

After completing this FY course, students will be able to:

- Understand the physical and virtual WCSU campus.
- Identify university community resources, including faculty, staff, and administration.
- Understand the necessary procedures that contribute to academic success and graduation at Western.
- Understand the culture and expectations of academics at the university level
- Understand habits and practices necessary for continuing academic success.

Course Content:

Unit 1: Early Ciphers (pre 700)

Unit 2: Mathematics Enters the Fray (700 to 1400)

Unit 3: Renaissance and Revolution Cryptology Moves West (1400 to 1700)

Unit 4: Enlightenment and Revolution (1700 to 1846-ish)

Unit 5: First Steps Toward Modern Ciphers (1846-ish to 1945)

Course Calendar:

Tuesday	Friday
8/28 **1** Syllabus, Intrroductions, Your First Cipher	8/31 **2** Simple Early Ciphers
9/4 **3** Arabic Numerical Ciphers, *Syllabus Quiz*	9/7 **4** Arabic Numerical Ciphers (continued), *Reading Quiz pp. 1-14*
9/11 **5** Cipher Practice, *Vocab Quiz (bring in flash cards)*	9/14 **6** **Group Exam I**
9/18 **7** Arabic Analysis of the Alphabet	9/21 **8** Falconer's Approach, *Reading Quiz pp. 14-25*
9/25 **9** Falconer's Approach (continued) FY Assign.: 1st Article Reflection	9/28 **10** Practice Analysis, *Reading and Vocab Quiz, pp. 26-44 (bring in flash cards)*
10/2 **11** **Group Exam 2** FY Assign.: 1st Schedule Tracking	10/5 **12** Alberti's Great Idea

Tuesday	Friday
10/9 **13** An Automatic Hit, *Reading Quiz pp. 45-63* FY Assign.: 2nd Article Reflection	10/12 **14** Presidential Secrets
10/16 **15** Stirring Things Up FY Assign.: Office Hours Sheet	10/19 **16** Cipher Practice, *Vocab Quiz (bring in flash cards)*
10/23 **17** **Group Exam 3**	10/26 **18** Registration and Stuff
10/30 **19** A Simple Solution FY Assign.: 2nd Schedule Tracking	11/2 **20** A Seventeenth Century Idea
11/6 **21** Nineteenth Century Revelations, *Reading Quiz pp. 63-82(top)* FY Assign.: 3rd Article Reflection	11/9 **22** Practice Analysis, *Vocab Quiz (bring in flash cards)*
11/13 **23** **Group Exam 4**	11/16 **24** Affine Ciphers
11/20 **25** Hill's Cipher, *Reading Quiz pp. 101-127* FY Assign.: 4th Article Reflection	11/23 Thanksgiving Recess - No Classes
11/27 **26** Enigma	11/30 **27** Alan Turing
12/4 **28** Cipher Practice, *Reading and Vocab Quiz, pp. 127-142 (bring in flash cards)*	12/7 **29** **Group Exam 5** FY Assign.: Final date for Cipher Chain

Grading:

Cryptology Assignments:

- **Vocabulary and Reading Quizzes:** You will have two of these per unit, and one quizzing your knowledge of the syllabus. These will be 10 minute quizzes checking to see that you have done the necessary reading and learned the vocabulary. (2% each × 11 = **22% of course grade**)

- **Group Cipher Exams:** You will have one of these for each unit. For these exams you will work in groups for one class period to encipher, decipher, and carry out cryptanalysis. (10% each × 5 = **50% of course grade**)

First Year Assignments:

- **Article Reflections:** You need to write up your thoughts on some articles, which I will give you, that discuss various aspect of how you can be a more successful student. This must be typed and submitted electronically in the appropriate folder within the network folder `X:\Dropoff\MAT\RoccaC`. Be sure to name your file in such a way that it is clear to whom it belongs and which assignment it represents without me needing to open it. (**4% of course grade**)

- **Office Hours Signature Page:** You must fill out your schedule including course title, meeting times, office hours, and instructor. Then you must visit each of your instructors during their office hours and have them sign off on the schedule. (**4% of course grade**)
- **Schedule Tracking:** The purpose of this is to help you figure out where your time is going and how you can best use your time to get the most from your education. For each of these you must also write a brief reflection on your schedule indicating where you think you could improve your time management. (**4% of course grade**)
- **Cipher Chain Resource Puzzle:** Each of you will be given a set of ciphers that you need to crack, but in order to do so you will need to hunt around both the physical campus and WCSU's website in order to find information which provides the key to the next cipher. (**8% of course grade**)
- **Note Taking:** The abundance of vocabulary and the nature of the algorithms inherent in this course make it imperative that you are well organized. Therefore, you will be required to take precise notes with separate sections of your notebook for rough class notes and neater revised notes. You will also be responsible for creating hand written flashcards for each vocabulary word. (**8% of course grade**)

Course Outline:

1. Ciphers
   (a) Monoalphabetic Ciphers
   (b) Polyalphabetic Ciphers
   (c) Specific Historical Examples: Caesar Shift, Arabic Arithmetical, Vigenere's Cipher, Thomas Jefferson's Cipher, Enigma
2. Historical Topics:
   (a) 500 B.C.E. (and before): Atabash, Scytale, Demaratus, Histiaeus
   (b) 50 B.C.E.: Caesar
   (c) 700-1000: Arab Cryptology
   (d) 1400-1850: Foiling Frequencies: Alberti's, Vigenere's , Jefferson's, and Playfair's Ciphers
   (e) 1790: Thomas Jefferson's Cipher Wheel / WWI M-94 Cipher
   (f) 1846: Babbage / Kasiski Test
   (g) 1934: ENIGMA in the service of the German Military
   (h) 1943: Colossus - The Birth of Computers
3. First Year Content
   (a) Student Habits of Mind and Body
      i. Importance of Note Taking
      ii. Time Management
      iii. Taking Care of Yourself
      iv. Getting Involved
      v. Making Contact
   (b) On Ground Resources
      i. Advisors and Professors
      ii. Tutoring
      iii. Information
      iv. Counseling
      v. Events
   (c) On-line Resources
      i. What's on at Western
      ii. Program Sheets
      iii. Advisor
      iv. Library Resources
      v. Banner

You and Your Grades:

- “A” (Exceptional) range 90% to 100%:
  The student has demonstrated significant mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and most nonstandard problems which require deeper insight.

  – “A” $\Longleftrightarrow 92.5\% \leq \mathit{Grade} \leq 100\%$

  – “A-” $\Longleftrightarrow 90\% \leq \mathit{Grade} < 92.5\%$

- “B” (Good) range 80% to 90%:
  The student has demonstrated mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and some nonstandard problems which require deeper insight.

  – “B+”$\Longleftrightarrow 87.5\% \leq \mathit{Grade} < 90\%$

  – “B” $\Longleftrightarrow 82.5\% \leq \mathit{Grade} < 87.5\%$

  – “B-”$\Longleftrightarrow 80\% \leq \mathit{Grade} < 82.5\%$

- “C” (Adequate) range 70% to 80%:
  The student has demonstrated adequate mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve most standard formulaic exercises but struggles with nonstandard problems which require deeper insight.

  – “C+”$\Longleftrightarrow 77.5\% \leq \mathit{Grade} < 80\%$

  – “C”$\Longleftrightarrow 72.5\% \leq \mathit{Grade} < 77.5\%$

  – “C-”$\Longleftrightarrow 70\% \leq \mathit{Grade} < 72.5\%$

- “D” (Inadequate) range 60% to 70%:
  The student has demonstrated inadequate or incomplete mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve some standard formulaic exercises but few if any nonstandard problems which require deeper insight.

  – “D+”$\Longleftrightarrow 67.5\% \leq \mathit{Grade} < 70\%$

  – “D” $\Longleftrightarrow 62.5\% \leq \mathit{Grade} < 67.5\%$

  – “D-” $\Longleftrightarrow 60\% \leq \mathit{Grade} < 62.5\%$

- “F” (Unacceptable) below 60%:
  The student has demonstrated essentially no mastery of the appropriate knowledge and skills relevant to the course. The student is unable to solve most standard formulaic exercises and essentially no nonstandard problems which require deeper insight.

End User Agreement:

General Expectations: As a student in this class you are expected to:

- show up for every class on time, prepared to learn,
- actively participate in class,
- take notes in class,
- review your notes on a regular basis,
- check your university email every day,
- check the class website at least every other day, (http://sites.wcsu.edu/roccac)
- begin studying for exams in a timely fashion,
- ask questions in class,
- attend office hours,
- seek help in the math tutoring clinic, and
- complete assignments and readings on time.

Assignment Guidelines: (These apply to all out of class work.)

- Out of class assignments should always look neat, legible, and professional; they must be written on loose leaf college ruled paper or be typed.
- Messy work, work on crumpled papers, or on paper torn from a notebook will be rejected and counted as late.
- Whenever appropriate, answers on all assignments should be given in complete sentences. I should be able to tell what your answer means without re-reading the problem.
- An assignment is considered late after I have handed it back or gone over it in class. Late assignments are accepted but will receive at most 75% credit. Also, late assignments go to the absolute bottom of the stack of papers to be graded, all on time work is graded first.
- If you work on an assignment as part of a group, then there may be no more than three individuals in the group and you must hand in only one copy of the assignment with all your names on it; if you hand in multiple copies, I will deduct points.

Exam Makeup Policy: To qualify for a makeup exam you must have a valid reason for missing the exam and, if at all possible, let me know ahead of time that you are missing the exam. You will need to show up for class in person in order to arrange a time for the make up exam. If you do not have a valid reason, do not give prior notice when possible, or simply do not show up for an exam, you are not entitled to a makeup and will not be given one. If you fail to show up for your makeup exam, you will not be given a second opportunity.

The 2% Exception: Any assignment, quiz, or other piece of work which is ultimately worth no more then 2% of your final grade can not be made up or turned in late.

Time on Task: For all your classes you should be spending at least 2 hours working outside of the class for every 1 hour in the class. In particular for this class you should be doing 6 hours of work a week not including class time. Note that this is an average, if you are weak in the subject or under prepared you will need to spend more time on the class.

Attendance: There is no specific policy for attendance in this course. However please keep the following in mind:

- if you have three consecutive unexcused absences within the first half of the semester I am required to report to the University that you have stopped attending,
- some assignments may be started, if not completed, in class, and
- while most of the dates and assignments for the course will be posted on the website occasionally small assignments or quizzes may only be announced in class.

Also, if you come in late after I have taken attendance, then *you* are responsible for emailing me to let me know you were in class.

Devices: If you wish to have an electronic device in class to help with learning the material, recording notes, or recording lectures that is fine. Please make an attempt to be polite and professional, do not not use your device for personal reasons during class; that is the sort of behavior that can ruin things for everyone.

Academic Honesty: If on any assignment, quiz, or exam you turn in someone else's work as if it were your own you will receive a zero on that assignment, quiz, or exam. If you are caught doing this three times you will receive an F in the course and the Dean will be informed of your academic dishonesty.
(WCSU Honesty Policy: http://www.wcsu.edu/facultystaff/handbook/forms/honesty-policy.pdf)

Accommodations: If you have need of an accommodation for testing or note taking, please visit AccessAbility Services, located in White Hall 005 (http://www.wcsu.edu/accessability). They will give you an accommodation letter which you must bring to me as soon as possible.

MAT 198 - 01: First Year Seminar Office Hours Signature Sheet, Due 10/15/2018

You need to collect signatures from all of your instructors and you advisor in their office hours.

Course Title	Meeting Time	Office Hours	Instructor	Signature*

***Instructors please only sign off on this schedule during your scheduled office hours.**

MAT 198 - 01: First Year Seminar

Schedule Tracking Sheet I: 9/24/2018 - 9/30/2018, Due 10/2/2018

	Monday 9/24	Tuesday 9/25	Wednesday 9/26	Thursday 9/27	Friday 9/28	Saturday 9/29	Sunday 9/30
9 am							
10 am							
11 am							
12 pm							
1 pm							
2 pm							
3 pm							
4 pm							
5 pm							
6 pm							
7 pm							
8 pm							
9 pm							

MAT 198 - 01: First Year Seminar

Schedule Tracking Sheet II: 10/22 - 10/28, Due 10/30/2018

	Monday 10/22	Tuesday 10/23	Wednesday 10/24	Thursday 10/25	Friday 10/26	Saturday 10/27	Sunday 10/28
9 am							
10 am							
11 am							
12 pm							
1 pm							
2 pm							
3 pm							
4 pm							
5 pm							
6 pm							
7 pm							
8 pm							
9 pm							