Dr. Rocca

Email: roccac@wcsu.edu
Site: https://sites.wcsu.edu/roccac/
Telephone: (203) 867-9360

MAT 127: Intro to Cryptology

Meeting Time: W 2:30-5:00 pm in TBA
Grading: Standard A-F
Credits: 3
General Education: Quantitative Reasoning

Office Hours:

Office hours are on ground this semester. If you need to meet virtually, we can make an appointment to do so via my WebEx Virtual Office: Higgins 101-DV (https://westconn.webex.com/meet/roccac)

Monday: 1:00 pm - 2:00 pm

Tuesday: 1:00 pm - 2:00 pm

Wednesday: None

Thursday: 1:00 pm - 2:00 pm, 3:30 pm - 4:30 pm

Friday: 1:00 pm - 2:00 pm

or by appointment

Course Materials:

For this course you will need:

- "The Mathematics of Secrets" by Joshua Holden (ISBN-13: 978-0691183312)
- A notebook and calculator which you need to bring to each class.

Course Description and Outcomes:

When messages are sent over public media, such as the Internet, there is a need to protect (encrypt) the information contained in those messages from unauthorized viewers. And when your adversaries send messages you may have need to break into their secrets (decrypt). This course is an introduction to cryptology focusing on the mathematics used to encrypt and decrypt messages. This course satisfies the general education QR competency. Prerequisites: C or better in MAT 100 or appropriate placement score.
After completing this course students will be able to:

- Demonstrate an understanding of basic number theory and the application of some key theorems,
- Encipher and decipher messages using a variety of standard algorithms when they know the key,
- Analyze data about an enciphered message in order to glean information about the message, and
- Be able to apply what they have learned to break ciphers and read messages based on limited information.

Course Content:

Unit 1: Basic Ciphers: Monoalphabetic, Polyalphabetic, and Transposition Ciphers (Chapters 1-3)

Unit 2: Ciphers in the 20th Century: DES, AES, and the One-Time Pad (Chapters 4 & 5)

Unit 3: Mathematical Ciphers and Public-Key Cryptography (Chapters 6-8)

Assessments and Grades:

Your grade in this class will be a weighted average as follows:

- 75% 3 Unit Exams
- 25% Out of Class Assignments

Unit Exams (75%): Each unit exam is 25% of your grade. The first two will be one hour and fifteen minute exams covering the content from the unit as listed above. The third exam will be two and a half hours during final exam week; it will cover all the material listed above for unit 3 (75% of the exam) and material from the previous two units (25% of the exam). For the first two exams you will be able to do exam redos to raise your grade (see guidelines below).

Out of Class Assignments (25%): Throughout the semester you will be given a variety of mathematical and cryptological exercises to work on and hand in. You should expect about one assignment per chapter. Some chapters may require a second assignment if they are particularly heavy on content. Occasionally you will be able to start an assignment in class and finish it later to hand in.

Exam Redos: For each unit exam you will be allowed to redo some specific questions in order to earn back up to 40% of the points you lost. Which questions you redo and how many questions you redo will depend on how you did on the exam. Redos are due within one week of when the exams are handed back, you must turn in the original exam stapled on top of the redos, and for each question you redo you must include a sentence or two explaining what you did wrong.

Writing Math Exercise: In order to help you understand what it means to write up mathematics in a neat and professional manner, you are required to complete the ***Exercises in Writing Up Mathematics*** packet. After this is completed, you will be expected to use what you learned when writing up out of class work. This will be considered an out of class assignment.

Quality of Work Guidelines: All the out of class work you turn in must be neat and professional. Answers must be in complete sentences. The quality of your work on out of class work (assignments, projects, and redos) counts for up to 10% of your grade.

Class Calendar:

Wednesday	
1/22 Syllabus, Introductions, and Historical Overview	**1**
1/29 Multiplicative, Affine, Monoalphabetic Ciphers, and Modular Arithmetic	**2**
2/5 Frequency Analysis and Distribution of Characters	**3**
2/12 Hill's Cipher, Matrix Arithmetic, and Linear Equations	**4**
2/19 Homophonic and Polyalphabetic Ciphers	**5**
2/26 A Little Probability and the Index of Coincidence	**6**
3/5 Transposition Ciphers	**7**
3/12 Review and Unit 1 Exam	**8**
3/19 Spring Break	

Wednesday	
3/26 Feistel Ciphers and DES	**9**
4/2 DES Continued and AES continued	**10**
4/9 One-Time Pad and Perfect Secrecy	**11**
4/16 Review and Unit 2 Exam	**12**
4/23 More on Modular Arithmetic: Exponents, Orders, Inverses Modulo Primes, and Fermat's Little Theorem	**13**
4/30 Euler's ϕ-Function, Euler's Theorem, and Inverses Modulo Composites	**14**
5/7 Diffie-Hellman, RSA, ElGamal	**15**
5/14 Final Exam Week: Unit 3+ Exam	**16**

Course Outline:

While many of these topics could be explored at a very deep and mathematically detailed level, in this class we will focus on the basic concepts and algorithms and how they come together in the field of cryptology. Please note the order of topics on the outline does not indicate the order in which the topics are taught.

1. Mathematical Topics
   - (a) Number Theory
     - i. Modular Congruence
     - ii. Primes and Composites
     - iii. Greatest Common Divisors
     - iv. Chinese Remainder Theorem
     - v. Fermat's Little Theorem
     - vi. Euler's ϕ-function
     - vii. Euler's Theorem
   - (b) Probability
     - i. Sample Spaces
     - ii. Outcomes and Events
     - iii. Probability vs. Odds
     - iv. Conditional Probability
     - v. Bayes' Theorem
   - (c) Elliptic Curves
     - i. Adding Points - Visually
     - ii. Adding Points - A Little Algebra
       - A. Factors and Roots
       - B. Polynomial Division
     - iii. Arithmetic Modulo a Prime
2. Encryption Schemes
   - (a) Symmetric Ciphers
     - i. Shift Ciphers
     - ii. Monoalphabetic
     - iii. Affine Ciphers
     - iv. Polyalphabetic
     - v. Vigenere's Cipher
     - vi. Hill's Cipher
     - vii. Vernam's One-Time Pad
     - viii. Feistel
     - ix. DES
     - x. AES
   - (b) Asymmetric Ciphers
     - i. RSA
     - ii. Diffie-Hellmen
     - iii. El Gamal
3. Cryptanalysis
   - (a) Ciphertext Only
   - (b) Cribs
   - (c) Known Plain Text

End User Agreement:

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

- attend class and take notes,
- actively read material in each section, taking notes,
- review your notes on a regular basis,
- check your university email every day,
- check the class site **at least** every other day,
- begin studying for exams in a timely fashion,
- ask questions early and often,
- attend office hours,
- seek help in the math clinic, and
- complete assignments and readings on time.

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

- Work done outside of class must always look neat, legible, and professional, adhering to given guidelines. Work must be very neatly written or preferably typed. The quality of your work will be factored into your grade, up to 10%. In extreme cases work may be rejected and then counted as late.
- An assignment is considered late after I have handed it back or gone over it in class. Late assignments are accepted but may receive at most 75% credit. Late assignments go to the absolute bottom of the stack of papers to be graded; **all on time work is graded before any late work.**
- If you work on an assignment as part of a group, then there may be no more than three individuals in the group and all your names must be on the assignment. You should hand in only one copy of the work.
- All work must be submitted in the manner directed.

Email Etiquette Guidelines: When sending an email you must include the course number and semester in the subject line. For example, if you are taking MAT 314 in Fall 1592 then the the subject line should begin with "[MAT 314 Fall 1592]." Also, you should always begin with a salutation such as "Dear Dr. Rocca" and end with a closing such as "Sincerely, I. Newton."

Technology Use: You are free to use technology in the classroom to support the learning of the content, i.e. for note taking, recording, taking pictures of the board etc.. Technology use will be restricted if it becomes disruptive, a distraction, or invades others privacy.

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 meet with me 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: If a class has any quiz or class work which is ultimately worth no more then 2% of your final grade can not be made up.

Time on Task: As a 3 credit class you should expect to average 8.0 hours of work a week including class time. Some weeks you may get away with less and some may require more.

Attendance: Unless otherwise stated, there is no specific policy for attendance in this course. However, 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**.

Academic Honesty: If on any assignment, quiz, or exam you turn in someone else's work, regardless of the source, 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. (https://www.wcsu.edu/faculty-handbook/2019-2020/policies-pertaining-to-students/academic-honesty-policy/)

Accommodations: If you have need of an accommodation for testing or note taking, please visit AccessAbility Services, located in the HAAS Library room 406 (http://www.wcsu.edu/accessability).

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.
- "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.
- "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.

- "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.
- "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.

Inspire Your Professors:

What to do:

- Show up, on time, ready to learn.
- Ask, and try to answer, questions.
- Put in the time and do the scut work.
- Seek help when you need it, utilize the resources available to you.
- Be an active participant in class and in your own education.
- Be curious about everything and be here to learn.

What not to do:

- Don't ask "What is this good for?"
- Don't ask "Did I miss anything?"
- Don't say "I don't get *it*."
- Don't fiddle with your phone or computer.
- Don't wander in late and rush out early.
- Try not to repeat questions that have just been asked and answered, sometimes multiple times.
- Don't just grub for points.
- Don't be a passive passenger to your own education.