Cryptology

Quest University Canada Block 4, Spring 2017

> *What affected me most profoundly was the realization that the sciences of cryptography and mathematics are very elegant, pure sciences. I found that the ends for which these pure sciences are used are less elegant.* – Jim Sanborn

How do we send our own confidential information through secure channels, and how can we break codes to uncover the secret information of our adversaries? The mathematical field of cryptology is dedicated to answering such questions. In this course we will study breakthroughs in cryptology, from secret messages in the Ancient world and the Enigma cipher in World War II, to modern cryptosystems that facilitate online commerce. Along the way, you will develop a sophisticated understanding of how numbers interact and develop the ability to communicate messages secretly and mathematics clearly.

Learning Goals

After successfully completing this course you will:

1. understand the value of having different methods of encryption, including both private key and public key methods
2. identify multiple methods for encrypting and decrypting messages
3. understand how tools from mathematics are used to make and break cryptographic systems
4. analyze and evaluate the strengths and weaknesses of a given cryptographic system
5. construct and communicate rigorous mathematical arguments
6. connect the study of cryptology to significant events in history and the modern world
7. identify how cryptology is used in contemporary daily life
8. come to see yourself as a capable user of mathematics
9. value understanding *why* mathematical and quantitative concepts make sense
10. be able to read mathematical and quantitative texts independently for learning
11. understand the necessity of solving a variety of problems to gain understanding

Course Information

Tutor:	Dr. Sarah Mayes-Tang	Dates:	Block 4, Fall 2017
Office:	Academic Building 447	Time:	M-F 9-12
E-mail:	sarah.mayes-tang@questu.ca	Classroom:	Academic Building 205
Website:	`moodle.questu.ca`		

Course Topics

Throughout the course, you will encounter a variety of cryptographic systems. For each, you will work to understand how the system is used to communicate secret messages, evaluate the security of the system, and find ways of breaking the system. The development of course topics is approximately chronological, beginning with ancient systems and culminating in the systems that are currently used to keep our data safe. The systems that we study will fall into the following categories:

- Monoalphabetic substitution ciphers (e.g. Caesar shift, affine, keyphrase substitution)
- Polyalphabetic substitution ciphers (e.g. Vigenere, Enigma)
- Polygraphic substitution ciphers (e.g. Polybius, Hall)
- Advanced encryption standard
- Public key cryptography (e.g. RSA, Diffie-Hellman key exchange)

Course Text

For this course, we will be using *The Mathematics of Encryption* by Margaret B. Cozzens and Steven J. Miller, available at the University bookstore. There is also an electronic copy available through the AMS, but I recommend the paper version. The textbook is mandatory. Remember that downloading illegal copies is a violation of academic integrity.

Course Requirements

> *If I have made any valuable discoveries, it has been owing more to patient attention than to any other talents* - Sir Isaac Newton

To demonstrate achievement of the course Learning Goals, you will complete the following assessments.

- Kryptos Competition Preparation Project
- Kryptos 2017 (`https://www.cwu.edu/math/kryptos`)
- 2 Math Challenges
- 1 Case Study (analysis)
- Final Codebreaking Challenge
- Final Project (Exhibition Poster or Kryptos Study Guide contribution)

To pass the course, you must also complete daily homework and readings, positively contribute to the class, and demonstrate engagement in your learning goals.

Kryptos Codebreaking Competition

> *Properly handled, ciphers are a matter on which great things are decided.* –Elizebeth and William Friedman

Kryptos is an annual codebreaking challenge administered by Central Washington University. Kryptos 2017 will be held over the first weekend of the course, from 4pm on Friday April 13 through 4pm on Monday April 17. This provides the perfect opportunity to challenge your codebreaking skills.

The Kryptos competition involves breaking three ciphers. Each challenge will present you with some ciphertext. The goal is to discover the original English plaintext message. Clues to help break the cipher may be contained in the actual cipher text or in the details of the accompanying scenario.

Pay close attention to the Contest Rules listed on the Kryptos website (`https://www.cwu.edu/math/contest-rules`). Note that you may not discuss the challenges with any living person not on your team. It is incredibly important that you maintain the highest standards of integrity, as Quest's reputation is on the line. Any discussion of the challenges with those outside of your team will result in immediate course failure and a plagiarism report will be filed with the Chief Academic Officer.

You should email me the same solution as you submit to Kryptos at the time you submit it. If you are unable to solve either Challenges 1 or 2, you should prepare a summary of your team's efforts on the challenge and submit it to me by 9 am on Tuesday, April 18.

You will also complete an assessment of your own and your team members' contributions, due online at 9 am on Tuesday, April 18.

Kryptos Competition Preparation Project

In order to prepare for the Kryptos competition, you need to be familiar with as many different classical cryptosystems as possible. You also need to know how to recognize the systems used to encrypt a given ciphertext and research cryptosystems given limited information.

To help accomplish both of these goals, you will research a cryptosystem with your Kryptos team and present your results to the class in a 10-minute presentation and in a one-page information sheet.

Math Challenges

> *An elegantly executed proof is a poem in all but the form in which it is written.* –Morris Kline

Math Challenges will give you the opportunity to contemplate, struggle with, and conquer mathematical problems. The questions on these problem sets are challenging and will probably look quite different from those that you have encountered in previous mathematics classes. The process of working through problems in this course mimics mathematical discovery.

These assignments will also allow you to develop your mathematical writing skills. Writing clear mathematics is not only important in math classes: it will help to improve your critical thinking and your ability to communicate ideas from other fields clearly. I have high

expectations for your writing; please read the guidelines for these assignments. If you have questions about what I expect, please come and speak with me.

Case Study

Three may keep a secret if two of them are dead. –Ben Franklin

The case study will present a scenario that requires you to make a judgement about the suitability of various cryptographic systems for a given scenario. It will give you the opportunity to compare and evaluate a variety of cryptographic systems. You will work with other students to produce a report that clearly outlines your assessment and conclusion.

Further information about the assessment of the Case Study will be provided on the course website. Note that each student will be required to submit a Group Assessment Form for your group members at the time the assignment is due.

Final Project

No man would spend his time in such a profitless occupation as ciphers. –FP Gervais

Further details for the final project will be given in Week 3 of the course. Notice that, prior to the final project deadline, you will submit a Prospectus for your project on Day 12.

Final Codebreaking Challenge

Five or six weeks later, she asked me if I had deciphered the manuscript... I told her that I had. –Casanova

The last class of the block will be dedicated to one final group codebreaking challenge. More details will be given closer to the date of the assessment.

Daily Reading and Homework

The only way to learn mathematics is to do mathematics. –Paul Halmos

Every day of the course, you will be assigned a daily homework assignment, consisting of readings and problems. The daily homework assignments will build on what you have already seen on homeworks and in class, and introduce new ideas that we will delve into in future classes.

The ability to understand mathematical texts is an important skill for *any* future mathematical study. This skill is vital for at least three reasons.

1. **Future Learning**. When you need to learn a mathematical concept on your own, your main resources will be written.

2. **Efficiency**. In an ideal world we might try to discover all the mathematics by ourselves, but this would be impractical. The great abundance of mathematical writing available allows us to learn from the experts.

3. **Learning to Communicate**. Just as reading many stories makes you a better storyteller, reading a lot of mathematics makes you a better mathematical communicator.

The daily homework problems also serve a variety of purposes. They provide practice in problem solving, help prepare you for the course assessments, give you the opportunity to assess your understanding of the concepts in the reading, and provide a common basis for class discussions. Completion of the daily homework is essential for achieving the learning goals of the class and for being a valuable class contributor.

Each class will begin with a discussion of the problems on the daily homework, and student presentations of some of the problems. This portion of the class will be student-led, and I will stay very little to encourage ownership and understanding of the material.

I will be collecting your Daily Homework on certain unannounced days, so please be prepared to submit your assignments every day. If you write on your Daily Homework during class, you need to use a different color so that it is clear what you completed during class vs. before class. Preparation for class and presentations during homework discussions will play a significant role in determining the formative activities portion of your grade.

Contributions to Class

- **Actively participate in class discussions,** asking questions, offering comments, and listening carefully to what others say. If you have a question about something, please ask! There will likely be other people who have the same question. When a student makes a claim, you should always be able to give some response: either you agree, disagree with a reason, or don't understand something specific.
- **Be respectful of other class members and maintain a collaborative environment.** Contributing to a class discussion does not mean talking a lot. You should listen carefully to others' ideas and be careful about offering a critique. When you do object to others' ideas, be kind.
- **Be prepared for class.** You can only bring your best work to class when you are adequately prepared for class.
- **Note Taking.** I recommend that you use a binder to organize your notes, as there will be frequent in-class handouts and worksheets that would be difficult to corral into a notebook.

Academic Integrity

While googling a homework problem or trading solutions with a classmate may seem like good strategies for doing well in this class, these actions will prevent you from learning material, refining your problem-solving skills, and developing self-sufficiency and self-esteem.

The consequences for cheating are severe. *Any* blatant academic dishonesty will result in failure of the course and immediate reporting to the Chief Academic Officer.

The following actions are *not* considered cheating.

- Discussing questions from Math Challenge Assignments with classmates, building off of each others' ideas

- Using online resources to help you understand the content of the course or practice problems (e.g. problems that you do not submit)
- Working with others to complete Daily Homework

The following actions *are* considered cheating.

- Looking for solutions to Math Challenges online (e.g. by searching or posting on a message board).
- Copying the writing or explanations of mathematical work from someone else
- Collaborating with students not in your group for the Case Study
- Talking to someone not in your group about the Kryptos Competition
- Using others' words or ideas without properly citing them

These examples are not comprehensive; if you have questions about whether something is considered cheating, please speak with me first.

Grading

While grades are (one) measure of progress, they are not a measure of promise. – Francis Su

Group Assessments	
Kryptos Competition Preparation Project	10%
Kryptos Competition	20%
Case Study	10%
Final Codebreaking Challenge	10%
Individual Assessments	
Math Challenges	30%
Final Project	20%

After each group assessment I will ask for feedback from your group members about your participation, and individual contributions will be taken into account when grading. Every member of the class is expected to be engaged and prepared for each class. If you are not prepared for a class (e.g. by not doing the reading or completing the homework), I will deduct 3% from your final grade.

The course grading scale is:

A	93-100%	B	83-86%	C	73-76%
A-	90-92%	B-	80-82%	C-	70-72%
B+	87-89%	C+	77-79%	D	60-69%

Any student at Quest can request a narrative evaluation (e.g. a written paragraph) in addition to their letter grade in any course. A narrative evaluation will give you more comprehensive feedback that you can learn from and additional information to present employers and graduate schools. If you wish to take advantage of this option, you have until the end of the 6th day of a course to sign up on the Registrar's Office Portal site.

Disability Accommodations

If you have a disability for which you seek accommodation, please make sure to have registered with the Learning Commons, as specified in the Student Accommodation Policy (`http://www.questu.ca/pdfs/_uploads/content/student_accommodation_policy.pdf`), and provide me with your Memorandum by the second day of class.

Due Dates

Unless otherwise noted, all assignments are due at the beginning of class (9 a.m.), and all deadlines are absolutely firm. I will not accept late homework since we need to be able to discuss solutions in class, and because staying on top of deadlines encourages you to keep up with course material. If you are late for class, your assignment will be considered late.

Please note the following important dates on your personal schedule.

Wednesday, April 12	Kryptos Preparation Project Due
April 14-April 17	Kryptos Competition
Tuesday, April 18	Summary of Kryptos Compeition Attempts Due
Friday, April 21	Math Challenge 1 Due
Monday, April 24	Case Study Due
Wednesday, April 26	Final Project Prospectus Due
Friday, April 28	Math Challenge 2 Due
Tuesday, May 2	Final Project Due
Wednesday, May 3	Final Codebreaking Challenge

Additional Course Policies

- I encourage you to work with others in the class to complete the Daily Homework, as explaining concepts to others is one of the best ways to increase your mathematical understanding. In fact, the workload in the course was determined with the expectation that you absolutely will work with others to complete the Daily Homework - it will be difficult to complete it on your own. You should be able to explain anything that you write down, and should not blindly copy the homework of others without discussing the problems.
- Please be on time to class. If you arrive for class and the door is closed this means that you are late. You will be permitted to be late 2 times without penalty during the block. On the third time, I will deduct 1% off of your final grade, and 1% more for each time that you are late.
- I expect that you will attend every class session. If you must miss a class for a valid reason (such as illness or a family emergency), please let me know *before* class. I reserve the right to ask for documentation to support your absence. For every class that you miss without a valid reason, 5% will be deducted from your *full* course grade.
- Bring pencils, paper, a scientific calculator, and a laptop to every class. You may also need to bring special materials such as scissors or pencil crayons to some classes, but will be given advanced notice when this is required.
- You cell phones must be off during class, and your laptops should be shut unless we are using them for a class activity.
- Always be respectful in your speaking and actions. Do not use profanity.
- If you need an extension on an assignment, I *must* see documentation, and you must place your request at least 24 hours ahead of the due date.

- Office hours: I hold open office hours regularly throughout the block; see the course website for the weekly schedule. If you drop by during an office hour and there is someone else in my office, come in! Students often learn most by listening to other students' questions. Note that office hours end promptly; if you plan to attend an office hour, come at least 15 minutes prior to the end time. If you need to speak with me privately, please e-mail me the weekend before to arrange an appointment.
- E-mail: During the block I check my e-mail on weekdays at the beginning and end of the day, and sporadically at other times. Please do not e-mail me with questions that may be easily answered by looking at this syllabus, the course website, or asking other members of the class. Be polite and use proper English grammar.
- Please do not bring food into the classroom. You may bring drinks.