**Math 360 - Mathematics of Information Security**
**Colorado State University**
**Fall 2023**

**General Class Information:**

| | |
|---|---|
| **Course Website:** | Canvas: https://canvas.colostate.edu// |
| **Dates:** | Aug 21 - Dec 10, 2023 |
| **Instructor:** | Dr. Cigole Thomas |
| **Email:** | cigole.thomas@colostate.edu, cigole@colostate.edu |
| **Class Time:** | MWF 10 am - 10:50 am MDT |
| **Office Hour Time:** | M 11-11:45 am, W 11 am - 12 pm and by appointment |
| **Class Location:** | Natural Resources, Room 109 |
| **Office Hour Location:** | Weber 219 |
| **Final Exam Date:** | Dec 14, Thursday 4:10 pm - 6:10 pm |
| **Computer Lab Location** | Weber 205 |

**Textbook:** Hoffstein, Pipher, Silverman, 2014, *An Introduction to Mathematical Cryptography*, Springer (free for CSU students through SpringerLink). Please use the link only once to download the book.

**Course Description:** Main topics covered in this class are the following:

1. Modular Arithmetic, Rings, Powers, Primitive roots, Prime numbers, Euclidean Algorithm, Chinese remainder theorem, Finite Fields
2. Ciphers, RSA and El-Gamal cryptosystems, Primality Testing, Pollard's $p-1$ factorization algorithm
3. (Time Permitting) Probability, Bayes's Formula, Random Variables, Monte-Carlo algorithm

**Prerequisites:** (MATH 156 or MATH 161) and (MATH 229 or DSCI 369 or MATH 369)

**Email Policy:** You are welcome to email me or come to the office hours if you have any questions about the course material. All emails must be sent through your official CSU student email account. Since I am teaching two different classes, include MATH 360 in the subject line to help me prioritize student emails and respond in a timely fashion.

**Canvas:** All the information regarding the class including syllabus, homeworks, grades and assignments will be posted on canvas. Check your email and canvas for announcements.

**Office hours:** The office hours for this class are Monday from 11 -11:45 am, Wednesday 11 am - 12 pm and by appointment. The office hours will be held in Weber 219. If you cannot make any of these times, email me and I will try to find an alternate time. Please come and talk to me if you have questions or you are struggling with the course material. I am here to help you and want all of you to succeed in this course.

**Grading Scheme:** Your grade will be weighted as follows.

| Category | Weight |
|---|---|
| Homework | 15% |
| Midterm 1 | 20% |
| Midterm 2 | 20% |
| Final Exam | 30% |
| Quiz | 15% |

**Homework:** There will be home work assigned through Canvas accessible under the tab 'Quizzes'. Group work is encouraged. You can ask me questions regarding homework. But all written answers should be yours without referring to others' or online solutions. All steps should be explained.

**Computer Labs:** There will be computer labs every other Friday starting the second week of classes. These will be held at Weber 205. The labs will allow you to practice the algorithms we learn in class. These are not graded and provided for your practice only. We will be using SAGEmath and instructions for each session will be provided.

**Quizzes:** There will be a quiz of 20 minutes at the beginning of class/computer labs based on the material taught in the two weeks preceding the day of the quiz. Make sure you arrive on-time for the quiz. Additional time will not be provided if you are late to the class. There won't be any makeups but I will drop the lowest grade to accomodate any unprecedented absences.

**Midterm Exams:** The Midterm Exams will be on October 2 (Monday) and 17 November (Friday). Make sure you can attend these dates. The duration is 50 minutes and each is weighted 20% of the total grade.

**Final Exam:** The final exam will be on Thursday, Dec 11 from 4:10 - 6:10 pm. See `https://registrar.colostate.edu/final-exams/` for the exam schedule. The final exam will be cumulative with more emphasis on material covered after the midterm.

**There will be no make-up for any of the exams** except for special circumstances (like a university excused absence or illness with a doctor's note).

**Note:** You need to show full work for full credit. Just writing the final answer will not suffice unless specified in the exam/quiz.

**Schedule:** A tentative schedule is attached on the last page. The exam dates will not change however the topics listed and the corresponding dates are subject to change.

**Calculators:** You may bring a calculator to the quizzes and exams.
(Calculator applications on phone/laptop/computer are not allowed).

## Help, Resources, and Important Information

**Accessibility:** If you are seeking accommodations for this class, you need to first contact the Student Disability Center. See the SDC website is `https://disabilitycenter.colostate.edu/` for detailed information. After discussing with SDC, then discuss your approved accommodations with me. Student Disability Center is located in TILT, room 121. Email: `sdc_csu@colostate.edu` | Phone: 970-491-6385

**Counselling Services:** (970) 491-6053; `https://health.colostate.edu/about-counseling-services/`.

**University Policies:** The University Catalog, `https://catalog.colostate.edu/general-catalog/policies/`, is the central resource for university policies affecting student, faculty, and staff conduct in university academic affairs. All members of the university community are responsible for knowing and following established policies.

**Academic Integrity Policy:** This course will adhere to the CSU Academic Integrity Policy as found on the Student' Responsibilities page of the CSU General Catalog and in the Student Conduct Code. At a minimum, violations will result in a grading penalty in this course and a report to the Office of Student Resolution Center. At minimum, academic integrity means that no one will use another's work as their own.
*CSU Honor Pledge:* "Academic integrity lies at the core of our common goal: to create an intellectually honest and rigorous community. Because academic integrity, and the personal and social integrity of which academic integrity is an integral part, is so central to our mission as students, teachers, scholars, and citizens, we will ask you to sign the CSU Honor Pledge as part of completing all of our major assignments."
"*I have not given, received, or used any unauthorized assistance.*"
Source: https://tilt.colostate.edu/integrity/pledge/.

**Important Dates:** See `https://catalog.colostate.edu/general-catalog/calendar/` for important dates relevant to Fall 2023.

| | MONDAY | WEDNESDAY | FRIDAY |
|---|---|---|---|
| 8/21/2023<br>**Week 1** | Syllabus<br>1.1 | 1.2 | 1.3 |
| 8/28/2023<br>**Week 2** | 1.4 | 1.5 | Computer Lab<br>Quiz 1 |
| 09/04/2023<br>**Week 3** | No Class | Catch up | 2.2 |
| 09/11/2023<br>**Week 4** | 2.3 | 2.4 | Computer Lab<br>Quiz 2 |
| 9/18/2023<br>**Week 5** | 2.4 | 2.5 | 2.5 |
| 9/25/2023<br>**Week 6** | 2.6 | 2.7 | Review<br>Quiz 3 |
| 10/02/2023<br>**Week 7** | MidTerm 1 | 2.8 | Computer Lab |
| 10/16/2023<br>**Week 9** | 3.1 | 3.1 | Catch up<br>Quiz 4 |
| 10/23/2023<br>**Week 10** | 3.2 | 3.2 | 3.3 |
| 10/30/2023<br>**Week 11** | 3.4 | 3.5 | Computer Lab<br>Quiz 5 |
| 11/06/2023<br>**Week 12** | 3.5 | 3.5 | 3.6 |
| 11/13/2023<br>**Week 13** | Catch up | Review | MidTerm 2 |
| 11/20/2023 | **No Class Fall break** | | |
| 11/27/2023<br>**Week 14** | 4.3 | 4.3 | 5.1 |
| 12/04/2023<br>**Week 15** | 5.3 | Review | Computer Lab<br>Quiz 6 |