**M/CS 478 Fundamentals of Cryptography Winter 2023**

---

**Instructor** Amites Sarkar

**Text** An Introduction to Mathematical Cryptography, 2nd edition
Hoffstein, Pipher and Silverman

**Preface**

This course is an introduction to mathematical cryptography. We'll cover the basic concepts and terminology of the subject, classical cryptosystems, elementary number theory and its application to the RSA and El-Gamal cryptosystems, Diffie-Helmann key exchange, and digital signature schemes. If time allows, we'll finish with an introduction to information theory and complexity.

**Syllabus**

I'll cover most of Chapters 1, 2 and 4, and selected sections from Chapters 3, 5, 7 and 8.

**Grading**

There will be three written homework assignments, each worth 20% of the final grade. These will all be due on **Thursdays**; specifically, **19 January, 9 February and 2 March**, and will all distributed in class and posted on the Canvas page, at least a week before they are due. The source material is class lectures and the textbook. You should bring your handwritten or (preferably) typed solutions to class. Solutions will be distributed in class and posted on Canvas, later.

For the presentations (20%), there will be 4 teams of 3 students, each tasked with giving a 30-minute presentation during the last week of the quarter (6–10 March). I'll talk more about this in class, and I'll post a list of possible presentation topics on Canvas.

The final (20%) will be comprehensive, and held from **1-3pm on Monday 13 March**.

To summarize, your final grade will be based on:

| | |
|---|---|
| Homework | 60% |
| Presentations | 20% |
| Final exam | 20% |

**Course objectives**

The successful student will demonstrate understanding of the following.

1. The basic concepts and terminology of cryptography and cryptanalysis.

2. Classical symmetric cryptosystems and methods for attacking them, and the ability to implement them.

3. Elementary number theory and the ability to apply it in the analysis of cryptosystems.

4. The Diffie-Hellman key exchange and the ElGamal and RSA asymmetric cryptosystems, and the ability to implement them.

5. The implementation, efficiency and security issues for cryptosystems considered.

6. Digital signature schemes related to cryptosystems considered, and the ability to implement them.

7. Basic information and complexity theory and the importance of hard mathematical problems in the design of cryptosystems.

**Academic honesty and student behavior**

I will uphold all aspects of Western's Academic Honesty Policy and Procedure, and the Student Rights and Responsibilities Code. See https://syllabi.wwu.edu for details, including academic honesty, special accommodations, etc.

In particular, excessive collaboration is not allowed. For example, you may discuss homework questions with other students in class, but you need to write your answers independently.

**Office hours**

My office hours are 1–1:50 on Mondays, Tuesdays and Thursdays, in 216 Bond Hall.
My phone number is 650 7569 and my email address is amites.sarkar@wwu.edu