M/CS 478 Fundamentals of Cryptography Winter 2021

Instructor	Amites Sarkar
Text	An Introduction to Mathematical Cryptography, 2nd edition Hoffstein, Pipher and Silverman

Preface

This course will take place online through Canvas and Zoom. My priorities are to make the course accessible, and the grading fair. The ideal way to participate is synchronously, at the regularly scheduled meeting time of 9am on Mondays, Tuesdays and Thursdays (I will host a Zoom meeting and invite everyone on the class list; **note that there will be no meetings on Fridays**). However, I will record each class meeting, and make the recordings available through Canvas, so it should be possible to complete the class asynchronously, if need be. The grading will be based on written homework, presentations, and a 10-minute oral exam during finals week.

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 four written homework assignments, each worth 15% of the final grade. These will all be due on **Tuesdays**; specifically, 19 January, 2 February, 16 February and 2 March, and will all be posted online on the Canvas page, at least a week before they are due. The source material is class lectures and the textbook. You should send me your solutions through Canvas, and I will provide feedback through Canvas.

For the presentations (20%), there will be 6 teams of 4 students, each tasked with giving a 30-minute presentation during the last week of the quarter (8–11 March). I'll talk more about this in class, and I'll post a list of possible presentation topics on Canvas.

For the final oral exam (20%), which will last for 10 minutes, you will give a 5-minute presentation (to me, not the whole class), and then answer questions for 5 minutes. The presentation will be on a topic chosen by you early in the quarter, and the questions will be directly related to your presentation, as well as to the course objectives (see below).

To summarize, your final grade will be based on:

Homework	60%
Presentations	20%
Oral 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 Advanced Encryption Standard and the underlying mathematics, and the ability to implement it.

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

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

8. 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 1–1:30 on Mondays, Tuesdays, Thursdays and Fridays, via Zoom.