MATH 3094: Mathematics of Encryption

Course Description:

Title: Mathematics of Encryption

Description:

Modern cryptography lies at the intersection of mathematics and computer science, involving number theory, algebra, algorithmic complexity, and potentially quantum mechanics. Many people think of codes in terms of spies, but in the information age, highly mathematical codes are used every day by almost everyone, whether at the bank ATM, at the supermarket, or when you send a text or purchase products online. Here is the same message encrypted in four different ways:

GUVF PBHEFR VF NJRFBZR (Caesar cipher)

DLGC GMEVQO MQ KACCSKO (Vigenère cipher)

OPGN NKLT KCBA BUSD ZDO (Enigma machine)

1062 338 184 774 649 324 350 693 1022 774 797 649 184 774 649 1002 812 797 774 350 21 797 (RSA, public key [1073, 5])

This course will provide a historical and mathematical tour of cryptography, from classical ciphers to quantum cryptography. The topics will include: classical ciphers (e.g., Caesar and Vigenère ciphers) and the attacks on them, the Enigma system, public-key RSA (including a complete mathematical proof that it works), detecting and correcting errors, primality testing and digital signatures, and elliptic curve cryptography (if time permits).

Prerequisites: MATH 3240 (Intro. to Number Theory) or instructor consent to substitute MATH 3240 by CSE 2500 (or a strong grade in 2710). Enrollment requires instructor permission.

Meets: Tuesdays and Thursdays, from 12:30pm – 1:45pm, at MONT 314 (also known as the “Pi classroom”!)

Homework, Quizzes:

Homework will be assigned and collected every other week. Homework will be graded on completion only. If you have questions about how to solve a problem, you should talk to me in office hours or ask questions in class. **Homework is due in class on the date listed below. Late homework will not be accepted.**

Homework:

The homework problem sets will be posted here:

1. **Homework set 1** (due Thursday, Feb 1st):
    - Section 1.1: 1.1, 1.2, 1.3, 1.4, 1.5,
    - Section 1.2: 1.7, 1.8, 1.9, 1.10.,
    - Section 1.3: 1.16, 1.17, 1.18, 1.22, 1.24 (note: in the first edition, the numbering is slightly different, and you should do 1.15, 1.16, 1.17, 1.21, 1.23 instead for Section 1.3)
2. **Homework set 2** (due Thursday, Feb 15th):
    - Section 1.4: 1.28, 1.30,

    - Section 1.5: 1.32, 1.34, 1.36,
    - Section 1.6: 1.39 OR 1.41,
    - Section 1.7: 1.42, 1.43, 1.44, 1.46.
3. **Homework set 3** (due Thursday, March 8th):
    - Section 2.2: 2.3, 2.4,
    - Section 2.3: 2.6,
    - Section 2.4: 2.8, 2.9, 2.10,
    - Section 2.5: 2.11, 2.12, 2.13, 2.14,
    - Section 2.6: 2.16,
    - Section 2.7: 2.17.

Class Grade:

The grade will be computed based on homework performance, class participation, and two exams and a final.

The total grade will be computed as follows: Prelim 1 (100 points), Prelim 2 (125 points), the final exam (175 points) and a lecture grade (150 points). The lecture grade will be based on homework and class participation.

- **MIDTERM 1**: Covers Chapters 1 and 2. In-class, February 22nd.
    - Highlights from Chapters 1 and 2.pdf.
    - Midterm 1 – Solutions.pdf.

Course Outline:

Week	Topics	Notes
1	1.1	
	1.2, 1.3	
2	1.4	
	1.5	
3	1.7	

	2.1, 2.2	Homework set #1 is due
4	2.3	
	2.4	
5	2.5	
	2.6, 2.7	Homework set #2 is due
6	Catch up/Review	
	EXAM 1 – Thursday, February 22nd	
7	3.1	
	3.2, 3.3	
8	3.4, 3.5	
	3.9, 3.10	Homework set #3 is due
9	**SPRING BREAK**	
	SPRING BREAK	
10	4.1, 4.2	
	4.3	

11	5.1, 5.2	
	5.3, 5.4	Homework set #4 is due
12	Catch up/Review	
	EXAM 2 – Thursday, April 5th	
13	6.1	
	6.2	Homework set #5 is due
14	6.3	
	6.4	
15	Ch 7 (Intro to Lattices)	
	Review	Homework set #6 is due