

Spring 2024

MATH 3410 / LGIC 2200, T Th 10:15 - 11:35 a.m. EST.

Discrete Mathematics II

Professor Andre Scedrov

Professor Scedrov's Office: DRL 4E6.

Professor Scedrov's Office Hours: Online by appointment.

Prerequisites

Math 3400 / Lgic 2100 or permission of the instructor.

Textbook

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman: "An Introduction to Mathematical Cryptography", Second edition, Springer, 2014.

Further References

Johannes A. Buchmann: "Introduction to Cryptography". Springer, Second Edition, 2004. Paperback. ISBN 9780387207568.

"Handbook of Applied Cryptography" by Menezes, van Oorschot, and Vanstone. CRC Press, Fifth Printing, 2001. ISBN: 0-8493-8523-7.

Topics Covered

Overview of Probability Theory: Probability Distribution, Random Variable, Conditional Probability, Bayes Theorem, Expected Value.

Basic Concepts of Cryptology: Substitution Ciphers, Permutation Ciphers, Vigenere Cipher, Rotor Machines, Attack Models. Symmetric Ciphers, Block Ciphers, One-Time Pad, Information-Theoretic Properties of One-Time Pad, Perfect Secrecy, Misuses of One-Time Pad, Malleability. Stream Ciphers, Linear Feedback Shift Register, Golomb's Randomness Postulates, Linear Complexity, Non-linear Filters, Knapsack Keystream Generator.

Introduction to Number Theory: Congruences, Chinese Remainder Theorem, Fermat's Little Theorem, Euler's Theorem, Modular Exponentiation by Repeated Squaring. Finite Fields. Splitting Fields. Quadratic Residues. Legendre Symbol. Jacobi Symbol. Law of Quadratic Reciprocity.

Public-Key Cryptosystems: Diffie-Hellman Key Exchange, Person-in-the Middle Attack. Discrete Logarithm. RSA Public-Key Cryptosystem. Attacks on RSA. ElGamal Public-Key Cryptosystem. Digital Signatures, Selective Forgery, Existential Forgery. Signature Schemes Based on RSA. Signature Schemes Based on Discrete Logarithm: ElGamal Signature Scheme, Digital Signature Algorithm (DSA).

Selected topics from modern cryptography and computer network security, including: Probabilistic Primality Testing, Euler Pseudoprimes, Solovay-Strassen Primality Test, Strong Pseudoprimes, Miller-Rabin Primality Test. Hash Functions.

### Basic Course Information

There will be two take-home midterms, the first one due in class on Tuesday, February 20, 2024 and the second one due in class on Tuesday, April 16, 2024. Each midterm will be worth 25% of the grade and will have at least a two-week lead time, during which there will be no homework.

The take-home final exam will be due Thursday, May 9, 2024 during the final exam period and will be worth 30% of the grade. The take-home final exam will also have at least a two-week lead time, during which there will be no homework. The take-home final exam will also include a 5-page written report on a topic of your choice related to the course and approved in advance by the instructor.

Most other weeks during the semester there will be homework, each time with at least one week lead time. Total homework will be worth 20% of the grade. One lowest score homework can be dropped.

First homework will be assigned on Tuesday, January 30, 2024 and it will be due in class on Tuesday, February 6, 2024.

First midterm will be assigned on Tuesday, February 6, 2024 and it will be due in class on Tuesday, February 20, 2024.