MATH 470 Communications and Cryptography

Tentative schedule

Fall 2022

This tentative schedule might be revised during the semester without notification. See the course website for the up-to-date schedule.

The purpose of this schedule is to provide information about what sections of the textbook are expected to be covered in this course and when they are expected to be covered in the lectures.

- Week 1 (Aug 25)

  1.1 Simple substitution ciphers

  1.2 Divisibility and greatest common divisor

- Week 2 (Aug 30, Sep 1)

  1.2 Divisibility and greatest common divisor

  1.3 Modular arithmetic

  1.4 Prime numbers, unique factorization, finite field

  1.5 Powers and primitive roots in finite fields

  Assignment 1 due Sep 1

- Week 3 (Sep 6, 8)

  1.5 Powers and primitive roots in finite fields

  1.7 Symmetric and asymmetric ciphers

  Assignment 2 due Sep 8

- Week 4 (Sep 13, 15)

  2.1 public keys

  2.2 Discrete Log problem

  2.3 Diffie-Hellman key exchange

  2.4 The Elgamal public key cryptosystem

  2.6 Hardness of discrete log

  Assignment 3 due Sep 15

- Week 5 (Sep 20, 22)

  2.7 Collision algorithm for the DLP

  2.8 Chinese Remainder Theorem

  2.9 Pohlig-Hellman algorithm

  Assignment 4 due Sep 22

- Week 6 (Sep 27, 29)

  2.9 Pohlig-Hellman algorithm

  3.1 Euler's formula and roots modulo pq

  Assignment 5 due Sep 29

- Week 7 (Oct 4, 6)

  First Midterm is on Oct 4

  3.1 Euler's formula and roots modulo pq

  3.2 RSA

- Week 8 (Oct 11, 13 (11 no class))

  Oct 11 Fall break, no class

  3.2 RSA

  3.3 Implementation and security issues

  3.4 Primality test

- Week 9 (Oct 18, 20)

  Assignment 6 due Oct 18

  3.4 Primality test

  3.5 Pollard's $p-1$ Factorization Algorithm

  3.6 Factorization and difference of squares

- Week 10 (Oct 25, 27)

  Assignment 7 due Oct 25

  3.7 Smooth numbers and sieves

  3.8 Index Calculus and discrete logarithms

- Week 11 (Nov 1, 3)

  Assignment 8 due Nov 1

  3.8 Index Calculus and discrete logarithms

  3.9 Quadratic residues and quadratic reciprocity

- Week 12 (Nov 8, 10)

  Assignment 9 due Nov 8

  3.10 Probabilistic encryption

  4.1 Digital signatures

  4.2 RSA digital signatures

  4.3 Elgamal digital signatures

  5.1 Basic principle of counting

- Week 13 (Nov 15, 17)

  Assignment 10 due Nov 15

  5.1 Basic principle of counting

  5.3 Probability

  Second Midterm is on Nov 17

- Week 14 (Nov 22, 24 (24 no class))

  5.3 Probability

  Nov 24 is Thanksgiving, no class

- Week 15 (Nov 29, Dec 1)

  5.4 Collision algorithms and Meet-in-the-Middle attacks

  5.5 Pollard's ρ method

  6.1 Elliptic curves

- Week 16 (Dec 6, 8 (8 no class))

  6.1 Elliptic curves

  6.2 Elliptic curves over finite fields

  6.3 The elliptic curve discrete logarithm problem

  6.4 Elliptic curve cryptography

  Dec 8 is Reading day, no class