

Lecture: 3:05–4:20p.m. Monday, Wednesday, Room: Engr 239.

Instructor: Dr. Seung H. Son <http://www.uccs.edu/sson> E-mail: sson@uccs.edu

Office: Engr 282 Phone: [719] 255–3515 Fax: [719] 255–3605

1420 Austin Bluffs Parkway, Colorado Springs, Colorado 80933-7150.

Office hours : 12:30–1:30pm, 4:30-5:30pm Monday, or by appointment

Prerequisite: Math 414 (Modern Algebra I: groups, rings, fields, homomorphisms, polynomials, etc.)

Text: There is no set text for this course.

Reference: The Mathematics of Coding Theory, Paul Garrett, Online drafts,

or Book: 2004 Pearson Education, Inc., ISBN 0-13-101967-8, ISBN13: 978-0-13-101967-6.

Description: The basic ideas of the theory of error-correcting codes are presented. We will study some important examples and give applications. These codes are important for the digital transmission of data.

Important Dates:

Jan. 21 First day of lectures

Feb. 4 Last day to register/Final day for 100% Drop Refund

March 23–29 Spring Break: No classes

May 11 Last day of lectures

Exams: There will be three 75-minute in-class exams and a take-home final exam.

Exam 1 3:05–4:20p.m., Feb. 4 (Wed.)

Exam 2 3:05–4:20p.m., March 4 (Wed.)

Exam 3 3:05–4:20p.m., April 22 (Wed.)

Final Exam due 5p.m., May 18 (Mon.)

There will be NO makeup exams unless arrangements have been made prior to Feb. 5th. A missed exam will count as a **zero** toward your course grade.

Electronic devices: I will allow **NO electronic devices such as calculators, cell phones, etc.** for any exam. You must turn off your devices before the exam begins.

Grade : $3 \times 20\% + 10\% + 30\% = 100\%$

60%: 3 Midterm exams: 20%/each exam

10%: 10 best scores of quizzes (1%/each 1-min. pop-quiz)

30%: Final Exam

A: 93–100 A–: 90–92.9 B+: 87–89.9 B: 83–86.9 B–: 80–82.9 C+: 77–79.9

C: 73–76.9 C–: 70–72.9 D+: 67–69.9 D: 63–66.9 D–: 60–62.9 F: below 60%

If the mean/median/average is abnormally low, I may curve the grade.

Options: If your Quiz score average is over 80% on Feb. 5th, then your second exam score can override the first exam score.

Drop : Please seek counseling from the Dean's office before dropping *any* course.

April 3: Last day to drop without special permission from your Dean.

Disability Statement: If you have a disability for which you are requesting an accommodation, you are encouraged to contact the Disability Services Office within the first week of classes. The Disability Services Office is located in Main Hall #105. (Phone number is 255-3354)

We may be faster or slower than this plan.

January

- 21: Overview, Conventional/Heuristic Coding, Huffman Coding
- 26: Reduction, Divisibility, Euclidean Algorithm, Modular Calculation, Fermat's Little Theorem, Binary Exponentiation, Chinese Remainder Theorem
- 28: Parity, CRC, Hamming [7,4] Code, RSA

February

- 2: Review
- 4: Exam 1
- 9: Probability, Theory of Experimental Designs
- 11: Linear Algebra
- 16: Modern Algebra Basics
- 18: Groups, Rings
- 23: Finite Fields
- 25: Polynomial Algebra, Primitive Polynomials

March

- 2: Review
- 4: Exam 2
- 9: Uncertainty, Entropy, Channel, Definitions, Theorems
- 11: Bounds for Codes, Sphere Packing Problem
- 16: Linear (Block) Codes
- 18: Cyclic Codes (Hamming codes)
- 30: Review

April

- 1: Polynomial codes (BCH Codes)
- 6: Reed-Solomon Codes
- 8: Algebraic Geometric Codes (Goppa codes)
- 13: Golay Codes
- 15: Perfect Codes (Uniformly Packed Codes)
- 20: Review
- 22: Exam 3
- 27: Concatenated Codes
- 29: Arithmetic Codes

May

- 4: Basic cryptography
- 6: Elliptic Curves
- 11: Review