Math 328: Introduction to Coding Theory and Cryptography Spring 2024
General Course Information

Professor: Noah Aydin **Office:** RBH 319 **Phone:** 5674 **E-mail**: aydinn@kenyon.edu
Class Times: TR: 8:10-9:30 am **Classroom:** Hayes 203
Student Hours: MWF 9:10-10am; TR 9:40-11 am; and by appointment. See my weekly schedule on my website
Course web page: http://www2.kenyon.edu/depts/math/aydin/teach/328
Textbooks:

1) Coding Theory and Cryptography The Essentials, D. R. Hankerson et al., 2nd ed,Marcel Dekker.
2) Introduction to Cryptography with Coding Theory, W. Trappe and L. C. Washington. 3rd ed, Pearson
Additional modules written by Prof. Aydin will be made available

Course Description and Objectives: The theory of error-correcting codes and cryptography are recent applications of algebra and discrete mathematics to information and communications systems. Students will learn the basic ideas of coding theory and cryptography, understand their mathematical foundations, and learn how mathematical tools can be used to devise useful error correcting codes and cryptographic systems. Since ideas from computational complexity theory are essential for cryptography, we will discuss basic principles of computational complexity as well. While coding theory is concerned with the reliability of communication, the main problem of cryptography is the security and privacy of communication. Applications of coding theory range from enabling the clear transmission of pictures from distant planets to quality of sound in compact disks and wireless communication. Cryptography is a key aspect of electronic security systems. With the ever increasing role of digital communication, online transactions, and the general dependence on electronic systems in modern life, the importance these fields grows each day. A selection of topics from these two disciplines will be discussed including basics of block coding, linear codes, Hamming codes, cyclic codes, BCH codes, symmetric-key and public-key cryptography, and digital signatures. Other topics may be included depending on the availability of time and the background and interests of the students. Each student will write a final research paper in a topic of their choice and present it to the class. Other than some basic linear algebra, the necessary mathematical background (mostly abstract algebra) will be covered within the course. Active learning methods will be used throughout the semester.

Learning Goals:

- Demonstrate understanding of the mathematical principles that are employed in the disciplines of coding theory and cryptography
- Explain the connections between mathematical facts and their applications in solving problems in coding theory and cryptography
- Explain the significance of computational complexity in the disciplines of coding theory and cryptography
- Understand the relationship between problems in mathematics and the computational complexity of their solutions by computers
- Recognize the limits of computational methods
- Create and communicate formal mathematical proofs
- Learn how to search for relevant publications in the literature
- Practice writing a formal mathematical paper

Grading and Evaluation Criteria:
Final grades will be determined based on the performance in the following components.

Component	Percentage
Written Homework	20
Quiz/Attendance/Participation/Enthusiasm	10
Midterm Project	10
Two Midterm Exams	35
Final Presentation	7
Final Paper	18

Class Format and Daily Reading. *Actively reading* the textbook *before* each lesson is a necessity. Some of the problems from the textbook will be assigned as homework and some for class presentations. There will be a homework set due most days. Come to class prepared to ask questions, present problems and participate in discussions. There will also be a number of quizzes, some may be announced in advance some not. There may not be enough time to cover all aspects of each topic during the class. You will still be held responsible for the material. Much of the learning will take place outside the classroom. I will be available for help. Make sure you utilize the office hours or make appointments to get help that you may need in a timely fashion.

Exams/Papers: Two midterm exams for the course are tentatively scheduled as Exam I: Thu Feb 13 (week 5), and Exam II: Thu April 9 (week 11). There will be two projects in the course. The first one will be before the spring break. The second one will serve as the final exam. In lieu of a final exam, you will choose a topic in coding theory or cryptography, write a paper on it and present it to the

class. The final paper will be due the at officially assigned final exam date for the course which is Thu May 9, 11:30 am. The final presentations will take place during the last week of the class. Check out the course web page with information about the project and start thinking about a possible topic early.

Attendance, Engagement and Tardiness: Active participation in class activities as part of your group is critical for your success in this course. You should be FULLY engaged and committed for your own learning. Hence, coming to class every day is critical. Being late to the class is disruptive. After one unexcused absence, each unexcused absence will lower your overall course grade by 1% where n is the number of unexcused absence. According to Math Dept's Class Attendance Policy, a total of 6 absences (whether excused or not) will result in expulsion from the course. Tardiness and walking out of the classroom are distracting for everyone. Unless there is a real emergency, please do not leave the classroom before the class is over. Two tardiness or leaving the room during the class will count as an unexcused absence. No make-up will be given for quizzes. For the midterm exams, a make up can only be given with a justified and documented excuse. *No work will be accepted late* unless approved in advance for a valid excuse. Your performance on quizzes together with your level of engagement, enthusiasm, and participation in class activities will make up a significant part of your course grade.

Academic Honesty: The rules set forth in the 2023-2024 Course Catalog apply to all aspects of this course.
In general, any work submitted for credit must result directly from your own understanding, thoughts, and ideas. Presenting the work of others as your own is strictly prohibited. You must follow the guidelines given in this document in general and mathematics department's guidelines for written homework in particular. Using chatGPT or other generative AI tools are prohibited for any of the assignments or exams in this course. If you have any questions, please ask your professor for clarification.

Accessibility and Accommodations: Students who anticipate they may need accommodations in this course because of the impact of a learning, physical, or psychological disability are encouraged to meet with me privately early in the semester to discuss their concerns. In addition, students must contact Student Accessibility and Support Services (SASS) (740-427-5453 or sass@kenyon.edu), as soon as possible, to verify their eligibility for reasonable academic accommodations. Though I am happy to help you in any way I can, I cannot make any special accommodations without proper authorization from the SASS staff. Except in extraordinary circumstances (and at the very start of the course), accommodations must be certified and discussed with me at least one week before they are to take effect.

Non-Discrimination, Civil Rights and Title IX Compliance

Kenyon College does not discriminate in its educational programs and activities on the basis of race, color, national origin, ancestry, sex, gender, gender identity, gender expression, sexual orientation, disability, age, religion, medical condition, veteran status, marital status, genetic information, or any other characteristic protected by institutional policy or state, local, or federal law. The requirement of non-discrimination in educational programs and activities extends to employment and admission. As a faculty member, I am deeply invested in the well-being of each student I teach. I am here to assist you with your work in this course. If you come to me with non-course-related concerns, I will do my best to help. However, it is important for you to know that *all faculty, are considered Mandated Reporters* of any incidents of harassment, discrimination, and intimate partner violence and stalking. Meaning, I must report any such discussion to the Civil Rights/Title IX coordinator. I cannot keep information involving sexual harassment, sexual misconduct, interpersonal violence, or any other form of harassment or discrimination based on a protected characteristic, confidential. The Health and Counseling Center, the College chaplains, and the staff at New Directions Domestic Abuse Shelter & Rape Crisis Center are confidential resources. For further information, please refer to the following Kenyon College policies: Discrimination, Sexual Misconduct & Harassment: Title IX, VAWA, Title VII. Civil Rights Policy ADA & Section 504 Student Grievance Procedures

Some Books on Coding Theory and Cryptography

Here is a list of some introductory and reference books on coding theory and cryptography (there are many other books on the subject)

1. Intro to Cryptography with Coding Theory, W Trappe & L. Washington, Prentice Hall, 0-13-061814-4
2. The Mathematics of Secrets, J. Holden, Princeton, 9780691183312
3. Introduction to the Theory of Error-Correcting Codes, V. Pless, John Wiley, 471190470
4. A first course in Coding Theory, R. Hill, Oxford, 0-19-8538030
5. Introduction to Cryptography, J. A. Buchmann, Springer, 0387950346
6. Fundamentals of Error-Correcting Codes, W. C. Huffman & V. Pless, Cambridge, 521782805
7. Applied Abstract Algebra, R. Lidl & G. Pilz, Springer, 0-387-98290-6
8. Introduction to Coding and Information Theory, S. Roman, Springer, 0-387947043
9. Introduction to Coding Theory, J. H. van Lint, Springer, 3540641335
10. The Theory of Error Correcting Codes, F. J. MacWilliams & N. J. Sloane, North-Holland, 0-444851933
11. Cryptography Theory and Practice, D. R. Stinson, and M. B. Paterson, 4th ed, CRC Press, 978-1-1381-9701-5
12. An intro to error correcting codes with applications, S. A. Vanstone & P. C. van Oorschot, Kluwer, 0792390172
13. Error Control Coding, 2nd ed, S. Lin & D. J. Costello, Prentice hall, 0130426725
14. Coding and Information Theory, S. Roman, Springer, 0-387-97812-7
15. Error Control Coding, P. Sweeney, John Wiley, 0-470-84356-X

16. Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, and S. Vanstone, CRC, 0-8493-8523-7
17. Practical Cryptography, N. Ferguson & B. Schneier, John Wiley, 0-471-22894-X
18. Modern Cryptography Theory and Practice, W. Mao, Prentice Hall, 0-13-066943-1
19. Quantum Computation and Quantum Information, M. Nielsen & I. Chuang, Cambridge, 0-521-63503-9
20. Intro to Coding Theory, 2nd ed, J. Bierbrauer, CRC Press, 978-1-4822-9980-9
21. The Theory of Information and Coding, R. McEliece, Cambridge, 0-521-83185-7
22. Applied Abstract Algebra, Joyner, Kreminski & Turisco, John Hopkins University, 0-8018-7822-5
23. Coding Theory and Cryptology, H. Niederreiter editor, World Scientific/Singapur U. Press, 981-238-132-5
24. Applications of Abstract Algebra with Maple and Matlab, Klima, Sigmon & Stitzinger, CRC, 1-58488-610-2
25. Quantum Computation and Quantum Information, M. A. Nielsen & I. L. Chuang, Cambridge, 0-521-63503-9
26. Making, Breaking Codes: An Intro to Cryptology, P. Garrett, Prentice Hall, 0-13-030360-0
27. Error Control Systems for Digital Communication and Storage, S. B. Wicker, Prentice Hall, 0-13-200809-2
28. Applied Cryptography, 2nd ed, B. Schneier, Wiley Press, 978-1-119-09672-6
29. Understanding Cryptography, C. Paar& J. Pelzl, Springer, 978-3-642-44649-8
30. Introduction to Cryptography, S. Padhye, A. Sahu,& V. Saraswat, CRC Press, 978-1-138-07153-7
31. The Mathematics of Encryption, M. Cozzens & S. Miller, AMS, 978-0-8218-8321-1
32. Coding Theory: A First Course, S. Ling, C. Xing, Cambridge University Press, 978-0521821919
33. Modern Cryptography and Elliptic Curves: A Beginner's Guide, T. R. Shemanske, AMS, 978-1-4704-3582-0
34. Cryptography, S. Rubinstein-Salzedo, Springer, 978-3-319-94817-1
35. A Course in Cryptography, H. Knospe, AMS, 9781470450557
36. A Course in Error-Correcting Codes, J. Justesen, T. Hoholdt, EMS, 3-03719-001-9
37. A Course in Algebraic Error-Correcting Codes, S. Ball, Birkhäuser, 978-3-030-41152-7
38. Public Key Cryptography: Applications & Attacks, L. M. Batten, Wiley, 9781118317129
39. Computer Security and Cryptography, A. G. Konheim, Wiley, 9780471947837
40. Modern Cryptography Primer, C. Koscielny, M. Kurkowski, M. Srebrny, Springer, 978-3-642-41385-8
41. An Intro to Mathmetaical Cryptography, J. Hoffstein, J. Pipher, J. Silverman, Springer, 978-1-4939-1711-2
42. Post Quantum Cryptography, D. Bernstein, J. Buchmann, E. Dahmen, Springer, 2009, 978-3-540-88701-0