Math 328: Introduction to Coding Theory and Cryptography Spring 2019
General Course Information

Professor: Noah Aydin **Office:** RBH 319 **Phone:** 5674 **E-mail**: aydinn@kenyon.edu
Class Times: TR: 2:40-4 pm **Classroom:** RBH 311
Office Hours: MWF 10:10-11; T&R: 4:30-5:30 and by appointment. See my weekly schedule on course web site.
Class 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. 2nd ed, Pearson

Course Description and Objectives: The theory of error-correcting codes and cryptography are two 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 principals 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 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.

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: Tue Feb 12 (week 5), and Exam II: Tue April 9 (week 11). There will be two projects in the course. The first one will be in the middle of the semester. 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 Wed May 8, 1:30 pm. 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. Frequent tardiness to the class will be considered as absence. No make-up exam will be given without justified and documented excuses. *No work will be accepted late*. Each unexcused absence will have a negative impact on your grade 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 2018-2019 Course Catalog apply to all aspects of this course. http://www.kenyon.edu/directories/offices-services/registrar/course-catalog-2/administrative-matters/academic-integrity-and-questions-of-plagiarism/
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. If you have any questions or uncertainty, please ask your professor for clarification.

Disabilities: If you have a disability which requires an accommodations in this class, please feel free to discuss your concern with me, but you should also consult Ms. Erin Salva, the coordinator of student access and support services (salvae@kenyon.edu, x5453). It is Ms. Salva who has the authority and expertise to decide on the accommodations that are proper for your disability. Though I am happy to help you in any way I can, I cannot grant any accommodations without a notification from Ms. Salva.

Title IX
Kenyon College seeks to provide an environment that is free of bias, discrimination, and harassment. If you have been the victim of sexual harassment/misconduct/assault, we encourage you to report this. If you report this to a faculty member, she or he is obligated to notify our college's Title IX coordinator about the basic facts of the incident (you may choose whether you or anyone involved is identified by name). The Title IX coordinator will assist you in connecting with all possible resources both on and off campus. Kenyon College's Title

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. Applied Abstract Algebra, D. Joyner, R. Kreminski & J. Turisco, John Hopkins 0-8018-7822-5
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, Chapman& Hall/CRC, 1584882069
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