**MAT 303: Cryptography and Coding Theory**
**Program Cover Document**

## I. Basic Course Information

MAT 303: Cryptography and Coding Theory is a one course unit, graded course that meets for two 80-minute periods each week. The course will introduce students to topics in the fields of cryptography and coding theory. The field of cryptography studies the secure communication of information, and the field of coding theory studies the design of efficient and reliable methods of transmitting data.

The course is an optional course for Mathematics majors. It will also be of interest to students in the Computer Science, Electrical Engineering, and Computer Engineering majors. The course is aimed at junior and senior students.

*Course Prerequisites*: The prerequisites are MAT 200 and MAT 205 (the MAT 200 prerequisite can be met with CSC 270 and permission from the chair)

*Course Description (for Bulletin):* A survey of the fields of cryptography and coding theory. Topics will be chosen from the fields of historical cryptography, public keycryptography, Diffie-Hellman, ElGamal, elliptic curve cryptography, elliptic curve factoring, hash functions, and error-correcting codes (Hamming codes, BCH codes, Reed-Solomon, algebraic geometric codes).

## II. Learning Goals

a. Content goals: Students will gain acquaintance with many basic topics in cryptography and coding theory. Students will learn about modular arithmetic, historical cryptography, public key-cryptography, Diffie-Hellman, ElGamal, elliptic curve cryptography, elliptic curve factoring, hash functions, and errorcorrecting codes (Hamming codes, BCH codes, Reed-Solomon, algebraic geometric codes). Other optional topics such as zero-knowledge proofs and quantum computers and cryptography may be covered at the instructor's discretion.
b. Performance goals: At the completion of the course, students should demonstrate knowledge of various cryptographic systems; methods of decrypting an encrypted message; and efficient, reliable methods of sending information.

## III. Student assessment

a. Assessment plan: Students will receive regular feedback on their work through the assignment of homework, quizzes, projects, presentations, and examinations.

The syllabus should clearly describe the schedule for these assessment tools and how they will be used to calculate grades.

b. Rationale: Through the use of regular feedback from homework, quizzes, projects, presentations and examinations, students will be able to see and correct their misunderstandings and improve their performance.
c. Methods and criteria: We will use the assessment of homework, quizzes, student presentations, and examinations to evaluate student accomplishment of the course learning goals. These assessment tools are similar to the manner in which students will need to use their knowledge in the future of and are an appropriate way to assess the accomplishment of course learning goals.

## IV. Learning activities

a. Summary of learning activities: Learning activities will consist of a combination of lectures, group work, student projects and presentations, and computer assignments. The specific choice will depend on the instructor. Outside of class, students are expected to do a significant amount of individual and group homework to achieve the learning goals. Students should be expected to use appropriate tools, including computer software, as well as concrete models or algorithms.
b. Calendar or outline: A guide to the organization of the course, a schedule of assessment tools, and a plan for the coverage of topics should be provided to the students. Homework, quizzes, and examinations should be spaced at appropriate intervals throughout the semester.
c. Rationale: By giving students a multitude of ways to learn and do mathematics, the learning activities promote a deeper mathematics understanding and contribute to the learning goals of these programs. A regular spacing of assessment tools insures that students receive continual regular feedback on their work.

**MAT 303: Cryptography**
**Fall 2024 Course Syllabus**

*"To Think Deeply About Simple Things."*
-Arnold E. Ross

*Instructor:* Prof. T. Hagedorn, hagedorn@tcnj.edu, x-3053, Office: SCP 240
*Course Times:* In SCP 229, MR: 2-3:20pm
*Office Hours:* (in-person, in SCP 240, tentative ): M: 11-11:50; W: 10-10:50; and Th: 12:30-1:20.
*Textbooks:* We are using Trappe and Washington, "Introduction to Cryptography with Coding Theory", 3rd edition, and Simon Singh's "The Code Book"

*Course Catalog Description:* Prerequisite: MAT 200 or (CSC 270 and the permission of the chair), and MAT 205. 1 course unit. Content: A survey of the fields of cryptography and coding theory. Topics will be chosen from the fields of historical cryptography, public key-cryptography, Diffie-Hellman, ElGamal, elliptic curve cryptography, elliptic curve factoring, hash functions, and error-correcting codes (Hamming codes, BCH codes, Reed-Solomon, algebraic geometric codes).

*Course Learning Goals:* Students will gain acquaintance with many basic topics in cryptography and coding theory. Students will learn about modular arithmetic, historical cryptography, public key-cryptography, Diffie-Hellman, ElGamal, elliptic curve cryptography, elliptic curve factoring, hash functions, error- correcting codes (Linear codes, Hamming codes), and lattice-based codes. Other optional topics such as zero-knowledge proofs and quantum computers and cryptography may be covered at the instructor's discretion.

At the completion of the course, students should demonstrate knowledge of various cryptographic systems; methods of decrypting an encrypted message; and efficient, reliable methods of sending information.

*Course Schedule:* This course meets for three hours each week. We will cover topics from Chapters 1-4, 9, 10, 21, 23, and 24 as indicated on the course schedule (see below).

*Tests, Homework and Quizzes:* There will be weekly homework assignments and quizzes. We will have two tests based on the class material, homework and quiz problems, and examples worked in class.

*Assessment:* Grades will be calculated based upon homework and quizzes (25%), class discussion participation (5%), tests (35%), and the final exam (35%). The professor reserves the right to adjust the number or type of assignments, and the grading formula, as needed, to accommodate changes in the course during the semester.

*Participation:* Every student is expected to regularly participate in this course. Students are expected to have reviewed past material, be prepared to engage in discussions during class, ask questions, present solutions to homework problems, and to participate in Perusall assignments.

*Website/Email:* All course information, announcements, and assignment/test grades will be posted on Canvas. It also contains information that may help you succeed in this course. I'll assume you are keeping up to date with its contents. Please email me with questions as they arise. My goal is to respond to emails with a day, but sometimes other obligations prevent this. If I haven't responded by the next class meeting, please speak to me in person.

*Absence Policy:* Makeup exams will only be given in extraordinary circumstances and only when the request has been made in advance of the exam. You should speak to me in person as soon as you believe that you will miss an exam. Emails received the night before the exam will not excuse you from the exam.

*Diversity and Inclusion:* The TCNJ community is composed of people with diverse backgrounds, perspectives, and experiences, and both the college and I are committed to diversity, equity, inclusion, access and belonging. The college's Campus Diversity Statement can be viewed at:
`https://diversity.tcnj.edu/campus-diversity-statement/`

In this course, I hope to introduce you to the amazing world of integral calculus. In our class, I want to create learning environment where everyone participates and which supports a diversity of thoughts, perspectives and experiences. Please contact me (in person or electronically) or submit anonymous feedback if you have any suggestions to improve the quality of the course. To help accomplish this:

- If you have a name and/or set of pronouns that differ from those that appear in your official TCNJ records, please let me know!
- If you feel like your performance in the class is being impacted by your experiences outside of class, please don't hesitate to come and talk with me. I want to be a resource for you.
- You should strive to honor and respect the diversity of your classmates.
- I (like many people) am still in the process of learning about diverse perspectives and identities. If something was said in class (by anyone, including me) that made you feel uncomfortable, please speak to me about it.

*Classroom Envrionment and Commitment to Student Success, Safety, and Well-Being:* The TCNJ community is dedicated to the success, safety and well-being of each student. TCNJ strictly follows key policies that govern all TCNJ community members rights and responsibilities in and out of the classroom. In addition, TCNJ has established several student support offices that can provide the support and resources to help students achieve their personal and professional goals and to promote health and well-being. You can find more information about these policies and resources at the "TCNJ Student Support Resources and Classroom Policies" webpage here: https://academicaffairs.tcnj.edu/tcnj-syllabus-resources/.

Students who anticipate and/or experience barriers in this course are encouraged to contact the instructor as early in the semester as possible. The Accessibility Resource Center (ARC) is available to facilitate the removal of barriers and to ensure reasonable accommodations. For more information about ARC, please visit: https://arc.tcnj.edu/.

*Additional Policies:* Please note that the "TCNJ Student Support Resources and Classroom Policies" webpage (`https://academicaffairs.tcnj.edu/tcnj-syllabus-resources/`) contains all of the relevant policies that govern the classroom. In particular, it covers TCNJ's academic integrity policy, attendance policy, tutoring, and the Center for Student Success, among others. I encourage you to read through the policies on this page.

*Liberal Learning Outcomes:* MAT 303: *Cryptography and Coding Theory* has a Quantitative Reasoning designation as part of the Liberal Learning program. Quantitative Reasoning courses have the following learning outcomes:

1. Students should understand quantitative reasoning so they can respond effectively to claims deriving from quantitative arguments.

2. Students will understand how real-world problems and social issues can be analyzed using the power and rigor of quantitative methods while also learning to recognize and articulate the limitations of these methods.
3. Students will be able to do all of the following: evaluate, interpret, and draw inferences from mathematical models such as algorithms, formulas, graphs, and tables.
4. Students will be able to use quantitative methods (such as algebra, geometry, statistics and computation) to solve problems.

*Mathematical Trivia:* 1729, 17, 28, 341, 561, 496, 8128, and 65537 are some of my favorite numbers. Newton, Leibniz, Fermat, Euler, and Gauss are some of my favorite mathematicians. .

**Fall 2024: Cryptography & Coding Theory Tentative Schedule**

| | Dates | Topics |
|---|---|---|
| *Week 1* | 8/29 (Thursday) | §1:Intro to Cryptography §2.1, 2.2: Shift & Affine Ciphers, Basic notions of number theory; Congruences |
| *Week 2* | 9/3 (Tuesday)<br>9/5 (Thursday) | More Congruences & Shift/Affine Ciphers §3.2 Extended Euclidean Algorithm<br>§2.3 The Vigenere Cipher |
| *Week 3* | 9/9 (Monday)<br>9/12 (Thursday) | §2.4, 2.5: Substitution Ciphers; Sherlock Holmes<br>§2.7 Enigma (and permutations) |
| *Week 4* | 9/16 (Monday)<br>9/19 (Thursday) | §4.1, 4.2 Binary Numbers and ASCII; One-Time Pads<br>§4.3, 4.4, 4.5 Multiple Uses of a One-Time Pad; Perfect Secrecy of a One-Time Pad; Indistinguishability and Security |
| *Week 5* | 9/23 (Monday)<br>9/26 (Thursday) | §3.5, 3.6 Modular Exponentiation; Fermat's and Euler's Theorems<br>§3.6, 9.1 Fermat's Theorem and Euler's Theorem; RSA |
| *Week 6* | 9/30 (Monday)<br>10/3 (Thursday) | **Test #1**<br>Attacks on RSA, Reading Assignment |
| *Week 7* | 10/7 (Monday)<br>10/10 (Thursday) | *Fall Break*<br>§9.2, 9.3—9.5, 14.2 Attacks on RSA; About RSA Primes and Factoring Integers |
| *Week 8* | 10/14 (Monday)<br>10/17 (Thursday) | §9.3—9.5 About RSA Primes and Factoring Integers<br>§9.6, 13.1 The Application to Treaty Verification; RSA Signatures |
| *Week 9* | 10/21 (Monday)<br>10/24 (Thursday) | §3.7 Primitive Roots<br>§10.1 Discrete Logarithms |
| *Week 10* | 10/28 (Monday)<br>10/31 (Thursday) | §10.4 Diffie-Hellman Key Exchange<br>§10.5, 13.2 The ElGamal Public Key Cryptosystem and Signatures; Happy Halloween! |
| *Week 11* | 11/4 (Monday)<br>11/7 (Thursday) | §21.1 Elliptic Curve Addition Law<br>§21.2 Elliptic Curves Mod p |
| *Week 12* | 11/11 (Monday)<br>11/14 (Thursday) | §21.5 Elliptic Curve Cryptosystems<br>§24.1 Introduction to Error Detecting and Error Correcting Codes |
| *Week 13* | 11/18 (Monday)<br>11/21 (Thursday) | §24.2 Error Correcting Codes<br>**Test #2** |
| *Week 14* | 11/25 (Monday)<br>11/28 (Thursday) | §24.4, 24.5: Linear and Hamming Codes<br>*Thanksgiving Break* |
| *Week 15* | 12/2 (Monday)<br>12/5 (Thursday) | §23. Lattice Methods<br>Review SPECIAL ACTIVITY or CATCH-UP: TBA |
| *Week 16* | 12/9-10<br>12/11-17 | *Reading Period*<br>Exam Period (Do not make vacation plans before exam schedule is posted) |