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.

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 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).

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 error-correcting 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.