

NUMBER THEORY & CRYPTOGRAPHY
CSCI 4560/8566
MATH 4560/8566

1.0 Course Description

- 1.1 Overview of Content and Purpose:** (3 hours) This course covers topics in number theory and secure communication. From number theory: Factorization of Integers, Congruence Arithmetic, Primitive Roots, and Quadratic Residues and Reciprocity. In the area of secure communication: Hashing Functions, Character, Block and Stream Ciphers and their Cryptanalysis. Private-Key Cryptosystems such as DES, and also Public-Key Cryptosystems such as RSA and El Gamal. Also Diffie-Hellman Key Exchange, Digital Signatures, Secret Sharing, and Zero-Knowledge Proofs.
- 1.2 For whom Intended:** This course is intended for upper-level undergraduate and graduate students who have an interest in the Algebra underlying Cryptography. The audience will consist of a mixture of students majoring in Computer Science, Mathematics, and Secondary Education with a Math Emphasis. It will be a required course for students majoring in Secondary Education with a Math Emphasis.
- 1.3 Prerequisite:** MATH 2230 or Math 2030.

2.0 Objectives

- 2.1 Performance Objectives for the Student:** The student will understand the basic concepts of number theory, be able to communicate and problem-solve mathematically, understand the basic methods of secure communication and cryptanalysis, understand the concepts of Public vs. Private Key, have a basic knowledge of the current cryptographic protocols and the issues involved.

3.0 Content and Organization

- 3.1 Topics:**
1. Background
 - a. Mathematical Induction
 - b. Complexity of Integer Operations
 2. Divisibility
 - a. Greatest Common Divisor
 - b. Euclidean Algorithm
 - c. Factorization Methods
 3. Congruence Arithmetic
 - a. Linear Congruences
 - b. Systems of Linear Congruences
 - c. Chinese Remainder Theorem
 4. Applications of Congruences
 - a. One-way Hash Functions
 5. Special Congruences
 - a. Fermat's Little Theorem
 - b. Pseudoprimes
 - c. Euler's Theorem and Euler's Phi Function
 6. Elementary Cryptography
 - a. Character, Block and Stream Ciphers

- b. Basic Linear Cryptanalysis
- 7. Current Cryptosystems
 - a. Symmetric Key Systems: DES
 - b. Public Key Cryptosystems: RSA, Knapsack Ciphers
- 8. Other Cryptographic Protocols and Applications
 - a. Key Exchange Algorithms
 - b. Digital Signatures
 - c. Secret Sharing
- 9. Primitive Roots
 - a. Primitive Roots for Primes
 - b. Index Arithmetic
- 10. Applications of Primitive Roots
 - a. Pseudorandom Numbers
 - b. Public Key Cryptosystems: El Gamal
- 11. Quadratic Residues
 - a. Residues and Non-residues
 - b. Quadratic Reciprocity
- 12. Applications of Quadratic Residues
 - a. Zero-Knowledge Proofs
- 13. Some Nonlinear Diophantine Equations
 - a. Pythagorean Triples
 - b. Fermat's Last Theorem

4.0 Teaching Methodology

- 4.1 **Methods to be Used:** This course will use classroom lectures and demonstrations.

5.0 Evaluation

- 5.1 **Basis for Evaluating Student Performance:** Students will be required to illustrate their understanding of the material and their problem-solving ability by submitting written problem sets each week. These problem sets will be evaluated in terms of correctness of solution and clarity of presentation. The type of problem required of the student will at times vary depending upon their situation: Graduate vs. Undergraduate, Secondary-Education vs. Computer Science vs. Mathematics.
Approx. 40%

Students will take three exams (including a final) that consist of an in-class and take-home portion. The in-class exams will consist of relatively quick problems. It will be primarily computational with a few theoretical questions. The take-home exams will consist of longer computational problems as well as more in-depth theoretical problems. In every case, there will be a portion of the exam devoted to more theoretical issues that will be required of Graduate Students and not of Undergraduate Students.
Approx. 30%

Students will turn in a project at the end of the semester. The nature of the project will depend upon the background of the student.
Approx. 30%
For example:

Secondary Education majors may create a Teaching Module

(perhaps a website) presenting a topic in number theory or cryptography for use with Junior High or High School students.

Computer Science majors may submit an implementation of a cryptographic protocol or an analysis of a widely/ commercially available implementation.

Mathematics majors may submit their own investigation of a mathematical problem, or a state-of-affairs detailing the current state of a problem and its history.

Undergraduate students and Graduate students will be graded on different scales.

- 5.2 Basis for Determining Final Grade:** Grades will be determined on the basis of written problem sets, written examinations and a project.
- 5.3 Grading Scale:** Grades will range from A to F. The particular scale will be determined by each instructor, and will be distributed on the first day of class.

6.0 Resource Material

- 6.1 Textbook(s) or Other Required Readings:** Rosen, K., *Elementary Number Theory and its applications*, Addison-Wesley-Longman, 5th Ed., 2001.
- Stinton, D., *Cryptography: Theory and Practice*, CRC Press, 1995.

6.2 Supplemental Reading (work-in-progress):

Books:

1. Schneider, B., *Applied Cryptography*, Wiley, 1996.
2. Pfleeger, C., *Security in Computing*, 2nd Ed., Prentice Hall, 1996.
3. Stallings, W., *Cryptography and Network Security: Principles and Practice*, 2nd Ed., Prentice Hall, 1998.

Articles:

DES

1. Landau, S., *Standing the Test of Time: The Data Encryption Standard*, Notices of the AMS, **47** (3), March 2000, 341-349.
2. Landau, S., *SCommunications Security for the Twenty-first Century: The Advanced Encryption Standard*, Notices of the AMS, **47** (4), April 2000, 450-459.
3. Schaefer, E., *A Simplified Data Encryption Standard Algorithm*, Cryptologia, **20** (1), January 1996, 77-84.