Math 296 **Special Topic: Cryptography** **Spring 2006**
Monday, Wednesday, Friday - 12:50 to 2:00 p.m.
PPHAC 113

Instructors:

Instructors:	Ben Coleman	Alicia Sevilla
Office:	PPHAC 214	PPHAC 217
Phone:	610-625-7781	610-861-1573
e-mail:	coleman@cs.moravian.edu	sevillaA@moravian.edu
Office Hours:	M W Th F 10:00 – 11:00 a.m. and by appointment	M W F 11:10 a.m.-12:10 p.m., 2 –2:30 p.m., and by appointment

Course Description: Cryptography is the study of how to disguise information in order to limit access. Traditionally, cryptography was used solely for military and government purposes, but today it has broader application in areas such as wireless networks, cable and satellite TV transmissions, and internet banking. In this course, we will take a historical perspective to discuss a variety of classical and modern methods of encrypting and decrypting information. We will carefully introduce the relevant mathematics, which includes topics on number theory, probability, and abstract algebra, as well as descriptions of algorithms and complexity theory. In addition to reading and homework assignments, students will work on in-class activities and use computer techniques when appropriate.

Prerequisites: Math 170 or permission of the instructors.

Course goals: After successful completion of this course you will be able to

- use common encryption and decryption techniques;
- explain and apply the mathematics used in a variety of classical and contemporary encryption techniques;
- formulate strategies to break codes applying standard attacks such as statistical analysis and techniques from number theory;

Text: *Making, Breaking Codes: An Introduction to Cryptography*, Paul Garrett, Prentice-Hall, 2001.

Topics Covered: We will cover most sections of chapters 1-13 of the textbook. Topics include:

- Simple Ciphers: the shift cipher, reduction/division algorithm, the one-time pad, the affine cipher.
- Probability: Counting, basic ideas, statistics of English, attacks on the affine cipher.
- Permutations: substitution ciphers, transposition ciphers, permutations and cycles, shuffles, block interleavers.
- A Serious Cipher: the Vigenere cipher: least common multiple and greatest common divisor of integers, Kasiski attack, expected values, Friedman attack.

- More Probability: generating functions, variance, standard deviation, Chebycheff's inequality, law of large numbers.
- Modern and Symmetric Ciphers: design goals, Data Encryption Standard, Advanced Encryption Standard.
- The Integers: divisibility, unique factorization, Euclidean algorithm, multiplicative inverses, computing inverses, equivalence relations, the integers modulo *m*, primitive roots, discrete logarithms,
- The Hill Cipher: Hill cipher operation, Hill cipher attacks
- Complexity: Big-Oh/little-oh notation, bit operations, probabilistic algorithms, complexity of algorithms, subexponential algorithms, Kolmogorov complexity, linear complexity, worst-case versus expected.
- Public-Key ciphers: trapdoors, the RSA cipher, Diffie-Hellman key exchange, ElGamal cipher, Knapsack ciphers.
- Prime numbers: Euclid's theorem, Prime Number theorem, primes in sequences, Chebycheff's theorem, sharpest asymptotics and the Riemann hypothesis.
- Roots mod *p*: Fermat's little theorem, factoring special expressions, Mersenne numbers, exponentiation algorithm, square roots mod *p*, higher roots mod *p*.
- Roots Mod Composites: Sun Ze's theorem, special systems, composite moduli, Hensel's lemma, square-root oracles, Euler's theorem, facts about primitive roots, Euler's criterion.

Homework Assignments: Daily reading and writing assignments will be given. You are expected to complete all assignments when due and to come to class prepared to answer and ask questions. Some assignments will be collected and graded. For ungraded written homework assignments, you are encouraged to work with a classmate if you wish, but all work to be handed in for grading must be done individually, unless otherwise explicitly stated on the assignment. The Academic Honesty Policy guidelines for Mathematics courses, which are attached, are to be followed.
Graded assignments must be turned in on the date due to be graded without penalty. No assignment will be accepted after graded papers have been returned to the students.

Class Attendance: Regular attendance is required of all students. Students are responsible for all work covered in class, and all assignments, even if absent from class. If you must miss more than one class the instructor should be notified. Hourly exams must be taken at the announced time; make-up exams will be given only in the case of illness or extreme emergency.

Examinations: There will be two in-class exams, and a final exam.

The tentative dates of the in-class exams are:

Friday February 10 **Wednesday March 22**

Group Projects: Students will work in groups of two or three students on a three-step project that will result in two class presentations and one paper. Each group will be assigned an encryption method to analyze and explain to the class on a first presentation. Then the group will prepare a second presentation to describe and explain possible attack methods for that encryption. The same group will also prepare a paper that will describe the encryption method and the attacks, and will include a careful description of the mathematics used in them and appropriate examples.

Help: You are encouraged to ask questions in class and to see Dr. Coleman or Dr. Sevilla for extra help when necessary. Do not wait until you are behind to seek help. It is very important to keep up with the class work. You are also encouraged to study with other students in the class. Giving and receiving explanations can be very helpful when doing non-graded homework and in preparation for exams. For hand-in assignments you may ask questions of the course instructors but should not consult anyone else.

Grades: Final grades will be based on homework assignments, two in-class exams, one paper, a final exam, and class participation as follows:

Final exam	15%
two in-class exams	20 % (10 % each)
one paper	10%
class presentations	15% (first 5%, second 10%)
homework assignments	40%

ACADEMIC HONESTY POLICY GUIDELINES

MATHEMATICS

The Mathematics and Computer Science Department supports and is governed by the ***Academic Honesty Policy of Moravian College*** as stated in the Moravian College Student Handbook. The following statements will help clarify the policies of members of the Mathematics faculty.

In all homework assignments that are to be graded, you may use your class notes and any books or library sources. When you use the ideas or thoughts of others, however, you must acknowledge the source. For graded homework assignments, you may not use a solution manual or the help, orally or in written form, of an individual other than your instructor. If you receive help from anyone other than your instructor or if you fail to reference your sources you will be violating the ***Academic Honesty Policy of Moravian College.*** For homework that is not to be graded, if you choose, you may work with your fellow students. You are responsible for understanding and being able to explain the solution of all assigned problems, both graded and ungraded.

All in-class or take-home tests and quizzes are to be completed by you alone without the aid of books, study sheets, or formula sheets unless specifically allowed by your instructor for a particular test.