Math 296 Special Topic: Cryptography Fall 2011

Class Meetings: Monday, Wednesday, and Friday, 11:45 a.m.– 12:55 p.m., PPHAC 235

Instructor: Dr. Alicia Sevilla

Office: PPHAC 217

Telephone: 610-861-1573 (office), 610-867-1787 (home)

E-mail: means01@moravian.edu;

Office hours: Monday, Wednesday, Friday, 11 a.m. – 11:30 a.m. and 2:30 p.m. – 3:30 p.m.

Textbook: Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer Science+Business Media, LLC, 2008

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 an 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 instructor.

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;

Topics Covered: We will cover most sections of chapters 1-5 of the textbook and some sections of chapters 6 and 7, if time permits. Topics include:

- An Introduction to Cryptography: Simple substitution ciphers, divisibility and greatest common divisors, modular arithmetic, prime numbers, unique factorization and finite fields, powers and primitive roots in finite fields, symmetric and asymmetric ciphers.
- Discrete Logarithms and Diffie-Hellman: Public key cryptography, the discrete logarithm problem, Diffie-Hellman key exchange, the ElGamal public key

cryptosystem, an overview of the theory of groups, order notation and algorithm complexity, a collision algorithm for the discrete logarithm problem.

- Integer Factorization and RSA: Euler's formula and roots modulo pq, the RSA public cryptosystem, implementation and security issues, primality testing, Pollard's $p - 1$ factorization algorithm, quadratic residues and quadratic reciprocity, probabilistic encryption.
- Combinatorics, Probability, and Information Theory: basic principles of counting, the Vigenère cipher, probability theory, collision algorithms and meet-in-the-miccle attacks.
- Elliptic Curves and Cryptography: elliptic curves, elliptic curves over finite fields, the elliptic curve discrete logarithmic problem, elliptic curve cryptography.
- Digital Signatures (as time permits)

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:

Wednesday October 5 **Wednesday November 16**

Group Project: Students will work in groups of two or three students on 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. 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)
group project (paper and presentation)	15%	
class participation	10%	
homework assignments	40%	

Accommodations: Students who wish to request accommodations in this class for a disability should contact Mr. Joseph Kempfer, Assistant Director of Learning Services for Disability Support, 1307 Main Street (extension 1510). Accommodations cannot be provided until authorization is received from the office of Learning Services.

Note: *This syllabus is a guideline for the course. It may be necessary to make changes during the semester. I will announce any changes in class.*

The following **Academic Honesty Policy Guidelines** are to be followed. Please read them carefully.

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.