CRYPTOGRAPHY
FALL 2018

Instructor: Lawrence D'Antonio
Office: G128E
Office Hours: W: 11:10-1200, M, Th: 8:00 – 8:30, 3:00-4:00
WEB PAGE: https://pages.ramapo.edu/~ldant/cryptography/cryptography.html
E-Mail: ldant@ramapo.edu
Phone: (201) 684-7714
Text: *An Introduction to Mathematical Cryptography*, 2nd Ed., by J. Hoffstein, J. Pipher and J. Silverman, Springer (UTM), 2014

COURSE DESCRIPTION

This course is an introduction to modern cryptography. In general, cryptography aims to construct efficient schemes achieving some desired functionality, even in an *adversarial* environment. For example, the most basic question in cryptography is that of secure communication across an insecure channel: Can Alice send a message to Bob so that Bob understands the message, but no eavesdropper does? How can Bob be sure that the message received was sent by Alice? Another question is that of secure computation in an insecure environment: Can a group of parties perform some distributed computation (e.g., coordinate an attack, or tally a vote), so that an adversary controlling the communication channels and some of the parties cannot disrupt the computation or learn extra information?

While cryptography is an ancient field, the emergence of *modern cryptography* in the last few decades is characterized by several important features distinguishing it from classical cryptography. For one thing, the availability of computers and the wide spread of networked information systems and the Web, has dramatically increased both the need for good cryptography, and the possibilities that it can offer. In addition to the classical military and national security applications, a wide scope of financial, legal, and social cryptographic applications has emerged, from using a credit card on-line or sending an encrypted email, to more ambitious goals of electronic commerce, electronic voting, contract-signing, database privacy, and so on. The most important characteristic of modern cryptography is its *rigorous, scientific approach*, based on firm complexity-theoretical foundations. In contrast to the classical approach based on ad-hoc solutions (design a scheme that seems very hard to break, and hope for the best), modern cryptography aims for specific, rigorously quantifiable security guarantees, based on precise mathematical definitions and provably secure protocols.

COURSE GOALS

- Students will master a broad range of computational skills, specifically advanced modular arithmetic, finite field arithmetic, and the arithmetic of elliptic curves over a finite field.
- Students will be able to implement (algorithmically) the cryptographic schemes listed above, as well as various related protocols.
- Students will understand when and why, based on rigorous mathematics and complexity analysis, these encryption schemes are valid and secure.

COURSE REQUIREMENTS

You will be graded on the following requirements. Note: there are no make ups for anything.

(1) There will be a combination of homework assignments and quizzes. The lowest of these grades will be dropped. The remaining assignments averaged together will account for 20% of your final grade.

(2) Two midterm exams. The approximate dates of these exams will be Monday, October 15 and Monday, November 19. Each exam will be worth 20% of your final grade.

(3) Final exam, which will be cumulative. This is scheduled for Monday, December 17 from 11:40 am – 3:00 pm. The final will be worth 25% of your final grade.

(4) Term paper. This will be a short paper (details given later) on some application of cryptography. Examples such as Bitcoin, DES, AES, or other appropriate topics. The paper will be worth 15% of your final grade.

COURSE OUTCOMES

The following are the outcomes for this class and what assignments are relevant for the assignment

Outcome	**Term Paper**	**Homework**	**Tests**
Outcome 1: Students will master a broad range of computational skills, specifically advanced modular arithmetic, finite field arithmetic, and the arithmetic of elliptic curves over a finite field.		X	X

Outcome 2: Students will be able to implement (algorithmically) the cryptographic schemes listed above, as well as various related protocols.		X	X
Outcome 3: Students will understand when and why, based on rigorous mathematics and complexity analysis, these encryption schemes are valid and secure.	X	X	X

COLLEGE and COURSE POLICIES

Attendance Policy: Students are expected to attend all classes. College policy states that "students must notify faculty within the first week of the course if they anticipate missing any classes due to religious observance". Those who are absent or late are still responsible for obtaining any missed lecture notes, announcements, hand-outs, etc. from a classmate.

E-mail Account: In accordance to College policy, students are responsible for keeping their Ramapo College e-mail accounts active. There will be both college and class announcements sent out to these accounts.

Policy on Academic Integrity: Students are expected to read and understand Ramapo College's academic integrity policy, which can be found online in the *College Catalog*. Members of the Ramapo College community are expected to be honest and forthright in their academic endeavors. Students who violate this policy will be required to meet with the faculty member and/or will be referred to the Office of the Provost.

Students with Disabilities: Any student who needs course adaptation or accommodations because of a documented disability that has been documented with the Office of Specialized Services should make an appointment with the instructor as soon as possible.

College Closings: For college closings and special announcements call (201) 236-2902 or sign up for "Alert Me Now".

School of Theoretical and Applied Science Office: Location G301, Tel. (201) 684-7734.

Course grading scale: 100%-93% A, 92%-90% A-, 89%-87% B+, 86%-83% B, 82%-80% B-, 79%-77% C+, 76%-73% C, 72%-70% C-, 69%-67% D+, 66%-60% D,59%-0% F.

COURSE CONTENTS

Below are listed the topics covered and the corresponding section from the text.

- Arithmetic in the Ring Z_n

1) Basic Modular Arithmetic
   - Substitution Ciphers
   - Arithmetic in the Ring Z_n
   - GCD and the Extended Euclidean Algorithm
   - Modular Inverses
   - Linear Congruence Cipher
   - Symmetric versus Asymmetric ciphers

2) Exponentiation in Z_n and the RSA Cryptosystem
   - Public Key Cryptography
   - Fast Exponentiation in Z_n
   - Euler Phi Function
   - Inversion of Exponential Maps
   - RSA Cryptosystem
   - Advanced Factoring Algorithms

3) Discrete Log ElGamal (DLEG) Cryptosystem
   - ElGamal Cryptosystem in General
   - Insecurity of ElGamal over $< Z_n, + >$
   - Discrete Log ElGamal (DLEG)
   - Diffie-Helman Key Exchange
   - ElGamal Signature Scheme

4) Elliptic Curve Cryptography
   - Introduction to Finite Fields
   - Arithmetic of Elliptic Curves
   - Elliptic Curve Cryptosystems
   - Elliptic Curve Factoring