MATH 2190: INTRODUCTION TO CRYPTOGRAPHY
SPRING 2017

Instructor: Felice Manganiello [manganm@clemson.edu]

Office: Martin O-22
Office Hours: TDB

Time: TTh 9:30am-10:45am
Room: Martin E-004
Exam: Wednesday (May 3rd) 8:00am-10:30am

Website: `http://www.math.clemson.edu/~manganm/teaching/math2190-s17/math2190-s17.html`

Text book:

Required:

- M. Cozzens and S.J. Miller, *The Mathematics of Encryption, an Elementary Introduction*, AMS (American Mathematical Society).

Further Readings

- J.A. Buchmann, *Introduction to Cryptography*, second edition, Springer.
- K. Martin, *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press.

Prerequisites: Calculus of One Variable I (MATH 1060) and freshman or sophomore standing.

Scope of the course: Cryptography or cryptology (from Greek kryptós, ”hidden, secret”; and graphein, ”writing”, or -logia, ”study”, respectively) is the practice and study of the techniques used for secure communication in the presence of third parties called adversaries.

We use cryptography every day and most of the time we do it passively. Lately we even hear about it in debates. Indeed in a world where cryptography is used properly, cyber attacks would not be the headline of the news.

In essence, cryptography concerns four main goals. They are:

- *message confidentiality* (or privacy): Only an authorized recipient should be able to extract the contents of the message from its encrypted form.
- *message integrity*: The recipient should be able to determine if the message has been altered.
- *sender authentication*: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) to validate claims from emitter or to validated the recipient expectations.
- *sender non-repudiation*: The emitter should not be able to deny sending the message.

We are going to learn about cryptography from a mathematical point of view and will be looking at its impact on society.

Learning outcomes: At the end of the course you will be able to: understand and perform encryption and decryption of messages using different cryptosystems, perform cryptoanalysis of well known cryptosystems, securely exchange keys over a public channel and constructing pseudo-random generators.

Course Topics: The following is a list of topics that will be included in the course (see Contents page of the text book):

(1) Historical introduction;
(2) Classical Cryptography;
(3) Enigma and Ultra;
(4) Classical Cryptography: Attacks;
(5) Symmetric Key Encryption;
(6) Public Key Encruption;
(7) Modern Cryptography;
(8) Primality Testing and Factorization.

Further topics will be considered during the course.

Homework: There will be one homework about every other week, and all must be completed to receive a grade for the course. Homework will be given on Thursdays and will have to be turned in on the following Thursday (or on the earliest following day of class). The modalities of turning in homework will be discussed in class. Note: homework will be penalized 50% for each day they are late. After two days, they will not be accepted. No exception.

Grading: The final grade will be calculated as follows:

Homeworks: 30% | Midterm 1: 20% | Midterm 2: 20% | Final exam: 30%

The two midterms (to be taken in class) and the final will likely be closed notes, closed books. They will consist of a set of problems on all the material taught up to the lecture preceding the exam.

In the computation of the grade, numbers will be rounded to an integer using the floor operator, e.g. floor(79.77)=79. The grade will follow the scheme

A	90-100
B	89-80
C	79-70
D	69-60
F	59-0

Policies:

- You are expected to come to class regularly. You are also expected to participate in class discussions and ask questions when you are confused. Finally, you are responsible for any material covered in classes you miss.
- Students are responsible to check periodically both the webpage and the Blackboard page of the course.
- Absent Professor Policy: If the instructor has not arrived within 15 minutes of the scheduled class time, you may assume that class has been canceled.

Plagiarism: I encourage you to consult with your colleagues when you are working on homework. However, you will not understand the material or do well on the exams unless the work that you turn in is ultimately your own. Therefore, you must write up your answers alone, and without looking at anything you wrote down while working with your group. The work you turn in must be your own.

You must cite everyone with whom you worked or consulted as well as any material (books and online resources other than the course books and lecture notes) that you used to solve the problem. You can help another student, but you must not show him your homework.

Any breach of this policy will be considered an act of plagiarism, and will be reported.

Accessibility statement: Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should 2 let the professor know, and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged - drop-ins will be seen if at all possible, but there could be a significant wait due to scheduled appointments. Students who receive Academic Access Letters are strongly encoud to request, obtain and present these to their professors as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester. You can access further information here: `http://www.clemson.edu/campus-life/campus-services/sds/`.

Academic integrity statement: As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a "high seminary of learning." Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form.
See also `http://www.clemson.edu/academics/academic-integrity`.

Instructors' attendance policy: Any exam that was scheduled at the time of a class cancellation due to inclement weather will be given at the next class meeting unless contacted by the instructor. Any assignments due at the time of a class cancellation due to inclement weather will be due at the next class meeting unless contacted by the instructor. Any extension or postponement of assignments or exams must be granted by the instructor via email or Blackboard within 24 hours of the weather related cancellation.

Title IX: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This policy is located at `http://www.clemson.edu/campus-life/campus-services/access/title-ix/`. Mr. Jerry Knighton is the Clemson University Title IX Coordinator. He also is the Director of Access and Equity. His office is located at 110 Holtzendorff Hall, 864.656.3184 (voice) or 864.656.0899 (TDD).