MAT 4930-008 – Fall 2014
Introduction to Cryptography and Coding Theory – 3 credit hours

Instructor: Dr. Dmytro Savchuk

Office: CMC 310 **Office Hours:** TR 10:50am – 12:20pm
Phone: (813)-974-4989 **Email:** savchuk@usf.edu

Course Meeting Times: TR 9:30am – 10:45pm, CMC 120

Course Webpage: http://savchuk.myweb.usf.edu/teaching/2014C_MAT4930_crypto_coding/

Prerequisite(s): MAS 3105 and MGF 3301

Course Topics: This course will introduce the students to fields of cryptography and coding theory. Cryptology combines the studies of cryptography, the creating of masked messages, and cryptanalysis, the unraveling of masked messages. Coding theory is the study of coding schemes used to detect and correct errors that occur during the data transmission. To study these symbiotic disciplines, the students will use some basic tools of linear algebra, abstract algebra, number theory, probability, and combinatorics.

Course Objectives: A goal of the course is to provide students with the necessary background for advanced study in cryptology and coding theory, as well as equipping them with tools required for applications in this field. Students will understand the basic principles behind classical and public key cryptosystems and basic cryptographic attacks. Students are expected to be able to implement studied cryptographic and coding schemes using computer algebra systems. Students will also develop skills in problem solving, programming, clear thinking, and logical reasoning.

Course Outcomes: Students are expected to be able to

- encrypt/decrypt messages using classical and public key cryptosystems, including substitution ciphers, block ciphers, RSA, and ElGamal
- conduct simple attacks on the classical cryptosystems
- use RSA and ElGamal digital signature
- code/decode messages using Linear codes
- obtain bounds on the efficiency of linear codes
- use the existing software to encrypt/decrypt messages
- write programs implementing studied cryptographic and coding schemes using computer algebra systems

Text: *Introduction to Cryptography with Coding Theory,* 2nd Edition, Prentice Hall, 2005, by Wade Trappe and Lawrence Washington. Errata is also available at http://www2.math.umd.edu/~lcw/book.html

Additional Resource: *Introduction to Algebraic Coding Theory with Gap,* 2008, by Sarah Adams. Available for free at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.150.4741

Course Grades: The university's +/- grading policy will be used in assigning course grades. If your overall percentage of total points falls into the following range, you will receive the corresponding grade:
97-100 (A+), 93-96 (A), 90-92 (A-), 87-89 (B+), 83-86 (B), 80-82 (B-),
77-79 (C+), 73-76 (C), 70-72 (C-), 67-69 (D+), 63-66 (D), 60-62 (D-), 0-59 (F).

Homework: A few problems will be assigned from each section covered. It will be due one or two class meetings after the section was covered. Late homework will **not** be accepted. Students are expected to work independently on all homework assignments. The homeworks will be posted at:
http://savchuk.myweb.usf.edu/teaching/2014C_MAT4930_crypto_coding/homeworks.html

Project: Each student will be assigned a project (e.g., research and implement certain cryptographic or coding scheme).

Exams: There will be 3 in-class tests and the final cumulative exam. The *tentative* dates for the exams are:
Exam 1: September 18 (Tueday, Week 4)
Exam 2: October 21 (Tuesday, Week 9)
Exam 3: November 25 (Tuesday, Week 14)
Final Exam: December 11 (Thursday, 7:30am – 9:30am, CMC 120)

Makeup Exams: *Makeup exams will be given at the discretion of the instructor*. Thorough documentation of the student's reason for missing an exam must be provided before a makeup will be considered.

Grading: Homework 15%; Midterm Exams 15% each, Project 20%, Final (cumulative) 20%

Attendance: Attendance is expected and will be checked periodically.

Contingency Course Plan: In the event of an emergency, it may be necessary for USF to suspend normal operations. During this time, USF may opt to continue delivery of instruction through methods that include but are not limited to: Blackboard, Elluminate, Skype, and email messaging and/or alternate scheduling. It is the responsibility of the student to monitor the main USF website, emails and MoBull messages for important information about the closure. For information about the continuation of instruction, students are directed to their individual blackboard course sites.

Retaining Records: You should keep all of your returned homework and exams until you receive your final grade. You will need these to demonstrate that a grade was incorrectly recorded, should that happen.

Miscellaneous Policies:

- *Please* do not hold conversations, either with your classmates or your cell phone, during the lecture sessions. (Turn your cell phone off and keep it out of sight at all times.)
- Cheating will **not** be tolerated. Please refer to the Undergraduate Catalog for clarification of the university policy on Academic Dishonesty.
- Students who must miss a class period due to a major religious observance must notify the instructor of this absence, in writing, by the end of the second week of classes.
- Any student with a disability is encouraged to meet privately with the instructor during the first week of classes to discuss accommodations. The student must bring a current Memorandum of Accommodations from the Office of Student Disability Services (SVC 1133). This is a prerequisite for receiving accommodations. Exam accommodations through SDS usually require two weeks advance notice.
  Note: If you need extra time on exams, you *must* make arrangements to take your exams with the SDS office. You *cannot* receive extra time if you choose to take your exams with the course instructor.
- You are encouraged to take notes during lectures, but your notes are not to be sold.
- All unauthorized recordings of class are prohibited. Recordings that accommodate individual student needs must be approved in advance and may be used for personal use during this semester *only*; redistribution is prohibited.
- S-U Policy: Students who want to take this course for a grade of S-U must sign the S-U contract no later than the end of the third week of classes. There will be **no** exceptions.
- A grade of "I" indicates incomplete work and will only be considered when most of the coursework has already been completed with a passing grade (C or better).

Tentative Schedule:

Week	Topics
1	Introduction. Classical Cryptosystems: 2.1 – 2.4, 2.7 – 2.12
2	Basic Number Theory: 3.1 – 3.4
3	Basic Number Theory: 3.5 – 3.8
4	FIRST EXAM; Public key cryptosystems: 6.1, 6.2;
5	Public key cryptosystems: 3.9, 6.3
6	Public key cryptosystems: 6.7
7	Discrete logarithms: 7.1,7.2
8	Discrete logarithms: 7.3,7.4,7.5
9	SECOND EXAM; Digital Signatures: 8.1, 8.2
10	Digital Signatures: 8.3, 8.4
11	Introduction to Coding Theory:18.1, 18.2
12	Bounds on General Codes: 18.3
13	Linear, Hamming Codes: 18.4, 18.5
14	THIRD EXAM
15	Golay Codes: 18.6; Cyclic Codes: 18.7
16	FINAL EXAM