

Syllabus: CIS 4362/MAT 5932

Introduction to Cryptology and Information Security

**Department of Mathematical Sciences
Charles E. Schmidt College of Science
Florida Atlantic University**

***Fall 2008. CIS 4362 (CRN 82418)/MAT 5932 (CRN #85576),
Introduction to Cryptology and Information Security, 3 credits.***

Instructor

Rainer Steinwandt, Office SE 280
Phone: (561) 297-3353
Email: rsteinwa@fau.edu

Class Time and Place

Monday, Wednesday and Friday: 2:00 – 2:50 p.m., FL 404.

Office Hours

Monday, Wednesday, Friday: 3:30 – 5:00 p.m. or by appointment. Also, feel free to just come to the office—whenever time permits, questions and discussions are welcome. (If there should be any timing conflicts, like inevitable meetings during regular office hours, this will be announced beforehand in class, whenever possible.)

Course Web Site

<http://www.math.fau.edu/~srainer/IntroCrypto2008/>

Required Text and Materials

The book *Cryptography. Theory and Practice* (Douglas R. Stinson, 3rd edition, Chapman & Hall/CRC, 2006) covers large parts of the course material. If supplementary material is needed, this will be distributed in class or on the course web site as needed.

Course Objectives

The course explains standard techniques for analyzing and designing different types of cryptographic schemes. At this, the main focus is on basic techniques for data encryption.

After completion of the course, you should be able to name and explain basic types of cryptographic tasks and basic attack techniques. You should be able to give examples of block ciphers and be able to explain how they work and in which way they are used. Similarly, you should be able to give examples and explain techniques used in public key encryption. After completion of the course, you should be able to explain and apply a number of standard techniques for factoring integers and computing discrete logarithms as needed in cryptanalysis.

Additional objective for MAT 5932:

After completion of MAT 5932 you should have developed a clear understanding of the mathematical techniques underlying the discussed algorithms, and you should have developed some intuition to what extent the discussed encryption techniques need further elaboration before being suitable for actual applications.

Lecture Schedule

The lecture covers the following topics. The exact time frame per item varies (also in dependence of previous knowledge of the course participants), but a typical time frame is three—four weeks per item.

1. *Classical Cryptography*: Kerckhoff’s principle; classes of attacks; shift, substitution and affine ciphers; permutation ciphers; stream ciphers; linear feedback shift registers; one time pad
2. *Block Ciphers*: substitution-permutation networks; DES and AES; modes of operation for block ciphers; building a cryptographic hash function from a block cipher
3. *Public Key Encryption*: RSA; primality testing; simple algorithms for factoring integers; ElGamal encryption; generic algorithms for computing discrete logarithms; basic idea of semantic security
4. *Other Cryptographic Tasks*: digital signing; key establishment; secret sharing; zero-knowledge proofs

Assessment Procedures

There will be three homework projects $\{H_1, H_2, H_3\}$ plus two exams X_1 and X_2 . The scheduled dates and maximum number of points for each of these items are given in the following table.

Item	Date	Max. points
H_1	Sep 15, 2008	20
X_1	Sep 29, 2008	25
H_2	Oct 10, 2008	20
H_3	Nov 3, 2008	20
X_2	Dec 1, 2008	35

Exams will be given in class or as take home exam. Homework projects and take home exams will be assigned in class at the date specified in the above table and collected on the date specified on the assignment. Late assignments will not be accepted and graded with 0 points. Both for the exams and for the homework assignments, the problems for CIS 4362 and MAT 5932 may differ. It will be clearly indicated to which of the two courses the assigned problems belong.

Your overall grade in the course is derived from your cumulative performance as follows:

1. The lowest number of points achieved in the items $\{H_1, H_2, H_3\}$ is dropped. The points from the remaining two items and of the two items $\{X_1, X_2\}$ are added, yielding a final number of points $0 \leq P \leq 100$.
2. Your grade is derived from P according to the following table.

Value of P	Grade
> 94	A
$> 90 - 94$	A-
$> 87 - 90$	B+
$> 83 - 87$	B
$> 80 - 83$	B-
$> 75 - 80$	C+
$> 65 - 75$	C
$> 60 - 65$	C-
$> 57 - 60$	D+
$> 53 - 57$	D
$\geq 50 - 53$	D-
< 50	F

Graded exams and homework projects will be returned in class or can be picked up during office hours at the instructor's office. At the end of the course, the final grades will, in anonymized form, be available in front of the instructor's office (room SE 280).

Please keep all your exams and documentation of homework projects, so that a possible disagreement about your grade can be resolved.

Make-up Tests and Extra Credit

If you cannot attend an exam or hand in a homework project in time due to a relevant reason like significant health problems or being involved in a major traffic accident, you can make up the respective assignment.

Extra credit work is not possible.

Course Procedure

The course is conducted in lecture/discussion style. As computers are a crucial tool in cryptanalysis, some homework projects may require the use of a computer. For these assignments, you can use the hardware platform and programming language of your choice.

Students with Disabilities

In compliance with the Americans with Disabilities Act (A.D.A.) – Students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca – SU 133 (561-297-3880), in Davie – MOD I (964-236-1222), or in Jupiter – SR 117 (561-799-8585) and follow all OSD procedures.

Incomplete Grades

A grade of *I* (incomplete) will only be given under certain conditions and in accordance with the academic policies and regulations put forward in FAU's *University Catalog*. The student has to show exceptional circumstances why requirements cannot be met. A request for an incomplete grade has to be made in writing with supporting documentation, where appropriate.

Classroom Etiquette and Academic Integrity

Please refer to FAU's *Student Handbook* (<http://www.fau.edu/handbook/boca.htm>).