

Syllabus: MAD 6478

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

Fall, 2005. MAD 6478, Cryptanalysis, 3 credits.

Instructor

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

Class Time and Place

Tuesday and Thursday: 12:30 – 1:50 p.m., SC 179.

Office Hours

Monday, Wednesday, Friday: 2:00 – 2:50 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/MAD6478.html>

Required Text and Materials

The book *Cryptanalysis of Number Theoretic Ciphers* (Samuel S. Wagstaff, Chapman & Hall/CRC, 2003) covers large parts of the course material. However, for some of the topics addressed, additional references will be used. This supplementary material will be distributed in class or on the course web site as needed.

Course Objectives

The course explains standard techniques used for analyzing and attacking different types of cryptographic schemes. After completion of the course, you should be able to explain and apply typical algorithms used for factoring integers or computing discrete logarithms.

Also you should be able to explain and apply analysis methods for symmetric ciphers like differential and linear analysis.

During the course you are supposed to learn which kind of attacks against asymmetric encryption and signature schemes can provably be excluded with available theoretical tools, and which type of attacks are not covered by commonly applied models. To this aim, you should be able to judge the potential of some “non-mathematical” attack techniques, e.g., based on the use of timing information or of special purpose hardware. Finally, after completion of the course you should be aware of problems that can arise when composing several cryptographic protocols.

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 two weeks per item.

1. Introduction: “Obvious” attacks on some classical ciphers and textbook schemes
2. Algorithms for computing discrete logarithms and factoring large integers
3. Improving security through the use of provable security
4. Beyond encryption: security requirements for different types of cryptographic schemes, e.g., for signing or key establishment
5. “Non-mathematical” attacks, e.g., using side channels or dedicated hardware
6. Techniques for analyzing block and stream ciphers
7. Attacks on protocol level
8. “Standalone security” vs. “composable security”

Assessment Procedures

There will be four short quizzes $\{Q_1, Q_2, Q_3, Q_4\}$, three homework projects $\{H_1, H_2, H_3\}$, and two hourly exams $\{X_1, X_2\}$. The scheduled dates and maximum number of points for each of these items are given in the following table.

Item	Date	Max. points
Q_1	Sep 8, 2005	20
H_1	Sep 13, 2005	40
Q_2	Sep 29, 2005	20
X_1	Oct 6, 2005	60
H_2	Oct 13, 2005	40
Q_3	Oct 25, 2005	20
H_3	Nov 10, 2005	40
Q_4	Nov 29, 2005	20
X_2	Dec 8, 2005	60

Exams and quizzes will be given in class. Homework projects will be assigned in class and collected on the date specified on the assignment. Late assignments will not be accepted and graded with 0 points.

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

1. The lowest number of points achieved in the four quizzes $\{Q_1, Q_2, Q_3, Q_4\}$ is dropped, and the points of the remaining three quizzes are added to form item X_3 .
2. The lowest number of points achieved in the items $\{X_1, X_2, X_3\}$ is dropped. The points from the remaining two items and the points achieved in the homework projects $\{H_1, H_2, H_3\}$ are added, yielding a final number of points $0 \leq P \leq 240$.
3. Denoting by M the maximal final number of points achieved in class (taken over all course participants), the grade is derived from P and M according to the following table.

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

Graded quizzes, 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 quizzes, 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 quiz due to a relevant reason like significant health problems or being involved in a major traffic accident, you can make up the respective exam or quiz.

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 will 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 *Graduate Policies and Procedures Manual* (see <http://www.fau.edu/academic/gradstud/pol.pdf>). 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 the guidelines for good practice in graduate education in FAU's *Graduate Policies and Procedures Manual* (see <http://www.fau.edu/academic/gradstud/pol.pdf>).