

# **Syllabus: MAD 6209**

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

***Spring, 2006. MAD 6209, Advanced Topics in Cryptology,  
3 credits.***

## ***Instructor***

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

## ***Class Time and Place***

Monday, Wednesday, Friday: 2:00 – 2:50 p.m., BU 112.

## ***Office Hours***

Monday, Wednesday, Friday: 10:00 – 11:30 a.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/MAD6209/MAD6209.html>

## ***Required Text and Materials***

There is no textbook. Most of the course material will be based on conference or journal articles. This material will be distributed in class or on the course web site as needed.

## ***Course Objectives***

The course assumes a basic familiarity with elementary cryptographic concepts and terminology. Basing on this, the course gives an introduction to some advanced cryptologic topics and tries to enable an understanding of these. After completion of this course, for at least one or two the addressed topics, you should be able to understand and explain a research paper in detail.

## Lecture Schedule

Where possible, suggestions of course participants for topics of interest will be taken into account. In any case, the list of topics covered includes those listed below. 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. (Combinatorial) group theory and cryptography, e.g., building on braid groups
2. Multivariate polynomials in cryptography
3. Protocols and security notions for (group) key establishment
4. Quantum cryptography
5. Simulatability-based security modeling, like the UC-framework

## Assessment Procedures

There will be two homework projects  $X_1$ ,  $X_2$  and one exam  $X_3$ . Both homework projects and the exam will be assigned in class and collected on the date specified on the assignment. Homework projects can include a presentation to be given in class. The scheduled assignment dates and maximum number of points for the items  $X_1$ ,  $X_2$  and  $X_3$  are listed in the following table.

Item	Date	Max. points
$X_1$	Feb 10, 2006	40
$X_2$	Mar 22, 2006	40
$X_3$	Apr 12, 2006	40

Homework projects or an exam returned after the specified deadline will not be accepted and graded with 0 points. Next to the above items, you receive a score  $X_0 \in \{0, 1, 2, \dots, 20\}$  reflecting your attendance and participation in class.

Both homework projects and the exam 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 be available at the instructor's office (room SE 280). Please keep your exam and documentation of homework projects, so that a possible disagreement about your grade can be resolved.

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

1. The lowest number of points achieved in the items  $X_1$ ,  $X_2$ ,  $X_3$  is dropped.
2. The points from the remaining two items and the score  $X_0$  are added, yielding a final number of points  $0 \leq P \leq 100$ .
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.

<b>Value of P</b>	<b>Grade</b>
> 94% of <i>M</i>	A
> 90% – 94% of <i>M</i>	A–
> 87% – 90% of <i>M</i>	B+
> 83% – 87% of <i>M</i>	B
> 80% – 83% of <i>M</i>	B–
> 75% – 80% of <i>M</i>	C+
> 65% – 75% of <i>M</i>	C
> 60% – 65% of <i>M</i>	C–
> 57% – 60% of <i>M</i>	D+
> 53% – 57% of <i>M</i>	D
≥ 50% – 53% of <i>M</i>	D–
<50 % of <i>M</i>	F

### ***Make-up Tests and Extra Credit***

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

Extra credit work is not possible.

### ***Course Procedure***

The course is conducted in lecture/discussion style. Further on, presentations that are to be prepared as part of a homework project will be given in class. As computers are a crucial tool in cryptography, a homework project may require the use of a computer. For such 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>).