Syllabus: MAD 6478

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

Spring, 2008. MAD 6478, Cryptanalysis, 3 credits.

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

Class Time and Place
Monday, Wednesday and Friday: 1:00 – 1:50 p.m., ED 111.

Office Hours
Monday, Wednesday, Friday: 2:30 – 4:00 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/MAD6478Spring08/

Required Text and Materials
The course will not follow a particular textbook, and necessary 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. A main focus of the course is on understanding the possibilities and limits of modern frameworks offering provable security guarantees. 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 on information about the
power consumption of a device. Finally, after completion of the course you should be
aware of problems that can arise when composing several cryptographic protocols.

**Lecture Schedule**

The lecture is supposed to cover 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 weeks per item.

1. Introduction: security issues with “textbook schemes”
2. Formalizing security requirements, constructions for provably secure encryption
   schemes with and without idealizing assumptions
3. Beyond encryption: Attack models for different types of cryptographic tasks, e.g.,
   for signature and (group) key establishment schemes
4. “Non-mathematical” attacks like timing attacks and differential power analysis
5. Attacks on the protocol level, secure composition of cryptographic protocols

**Assessment Procedure**

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Date</th>
<th>Max. points</th>
</tr>
</thead>
<tbody>
<tr>
<td>H_1</td>
<td>Feb 11, 2008</td>
<td>30</td>
</tr>
<tr>
<td>H_2</td>
<td>Mar 12, 2008</td>
<td>30</td>
</tr>
<tr>
<td>H_3</td>
<td>Apr 7, 2008</td>
<td>40</td>
</tr>
</tbody>
</table>

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 points from the items \(H_1, H_2, H_3\) 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.
<table>
<thead>
<tr>
<th>Value of $P$</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&gt; 94$</td>
<td>A</td>
</tr>
<tr>
<td>$&gt; 90 - 94$</td>
<td>A−</td>
</tr>
<tr>
<td>$&gt; 87 - 90$</td>
<td>B+</td>
</tr>
<tr>
<td>$&gt; 83 - 87$</td>
<td>B</td>
</tr>
<tr>
<td>$&gt; 80 - 83$</td>
<td>B−</td>
</tr>
<tr>
<td>$&gt; 75 - 80$</td>
<td>C+</td>
</tr>
<tr>
<td>$&gt; 65 - 75$</td>
<td>C</td>
</tr>
<tr>
<td>$&gt; 60 - 65$</td>
<td>C−</td>
</tr>
<tr>
<td>$&gt; 57 - 60$</td>
<td>D+</td>
</tr>
<tr>
<td>$&gt; 53 - 57$</td>
<td>D</td>
</tr>
<tr>
<td>$\geq 50 - 53$</td>
<td>D−</td>
</tr>
<tr>
<td>$&lt; 50$</td>
<td>F</td>
</tr>
</tbody>
</table>

Graded 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 homework projects, so that a possible disagreement about your grade can be resolved.

**Make-ups and Extra Credit**

If you cannot complete an assignment in due time to a relevant reason like significant health problems, 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 1 (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).