Implementation and Cryptanalysis of Cryptographic Systems
(MAD 6209)

When: MWF 11:00 – 11:50 am, starting Monday, January 9, 2012
Instructor: Thomas Eisenbarth
e-mail: teisenba@fau.edu, phone: (561) 297-0809, office: SE 266

Office hours: MWF 12:40 pm to 1:50 pm, or by appointment

Course description
The goal of this course is to work out real-world aspects of cryptography: What problems have to be considered when cryptography is to be used in practice. The course gives an overview of how to achieve security in programs and IT systems. We will implement and break cryptographic solutions and learn how to protect against practical attacks.

Covered topics include:

1. Understanding how security protocols use cryptography
2. Efficient and secure implementation techniques for common cryptographic algorithms
3. Understanding and performing attacks on implementations
4. Protecting against implementation attacks using common countermeasures
5. Theoretical leakage models and possible resulting solutions

After attending the course you will understand why popular cryptographic protocols have been designed the way they are. You will further know how to build secure and efficient implementations of cryptography. You will have learned how to perform basic attacks on cryptographic implementations, and how to prevent them. The course will provide an overview of the relevant topics of research in certain aspects of modern cryptology.

Target Audience:
This course targets graduate students interested in cryptography. It is suited for students planning to do research in cryptography or other security related fields such as trusted computing, network and OS security, or general IT security. The course is suited for students with a math, CS, or similar background.
Textbook
The course will not follow a particular text book. The Handbook of Applied Cryptography is recommended as a reference. Further material will be provided through Blackboard.


Background on Cryptography:


Grading
Grading is based on projects, one MidTerm exam and the final exam. Exams will be in-class, take-home or a mix of both. The weights for the final grade are as follows:

<table>
<thead>
<tr>
<th>Projects</th>
<th>30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>MidTerm Exam (Feb. 24)</td>
<td>30%</td>
</tr>
<tr>
<td>Final Exam (May 2)</td>
<td>40%</td>
</tr>
</tbody>
</table>

The grading scale will be no worse than the following:

<table>
<thead>
<tr>
<th>Cumulative Performance</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>55% - 65%</td>
<td>D</td>
</tr>
<tr>
<td>&lt;55%</td>
<td>F</td>
</tr>
</tbody>
</table>
Attendance Policy
Students should attend all lectures and actively participate in class. In order to enhance and maintain a productive atmosphere for education, personal communication devices, including cellphones and laptops, must be turned off during class.

Disability Policy
In compliance with the Americans with Disabilities Act (ADA), students who require special accommodation due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) -- in Boca Raton, SU 133 (561-297-3880); in Davie, MOD 1 (954-236-1222); in Jupiter, SR 117 (561-799-8585); or at the Treasure Coast, CO 128 (772-873-3305) - and follow all OSD procedures.

Honor Code Policy
Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see University Regulation 4.001 at:

This syllabus is subject to reasonable changes at the discretion of the instructor.