Syllabus:
MAD 5474 Introduction to Cryptology and Information Security

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

Spring 2013. MAD 5474 (CRN 25624) *Introduction to Cryptology and Information Security*

Instructor

Rainer Steinwandt, Office SE 218
Phone: (561) 297-3353
Email: rsteinwa@fau.edu

Prerequisites

Minimum Grade of C in *MAS 2103 Matrix Theory* and
Minimum Grade of C in *MAD 2502 Introduction to Computational Mathematics* and
Minimum Grade of C in *MAS 4301 Modern Algebra*

Class Time and Place

Tuesday and Thursday: 9:30–10:50 am, BU 207,
collocated with *CIS 4362 Cryptography and Information Security*

Office Hours

Tuesday and Thursday: 12:01pm–1:45pm or by appointment. Also, feel free to come to the office anytime—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://math.fau.edu/~srainer/IntroCryptoSpring13/

Required Text and Materials

The course will not be based on a specific textbook. Required course material will be provided in class or on the course web site as needed. Access to a textbook like Serge Vaudenay: *A Classical Introduction to Cryptography, Applications for Communications Security*, Springer, 2006 may be helpful, but is not necessary for completing assignments or following the course.

Course Objectives

The course provides an introduction to basic cryptographic techniques and the pertinent mathematical foundations. At the end of the course you should be acquainted with the concepts of block and stream ciphers, public key encryption, digital signatures, and key establishment. After completing this course you should also know and understand common examples and uses of such schemes, including the AES, RSA-OAEP, the Digital Signature Algorithm, and the basic Diffie-Hellman key establishment protocol. Moreover, at the end of the course you should have a basic understanding of how to formalize security requirements of an encryption scheme.

Lecture Schedule

The following is a list of topics to be covered. The exact time frame per item varies (also in

dependence on previous knowledge of the course participants), but a typical time frame is 2 to 3 weeks per item. Before the final exam, a review of the covered material will be provided.

1. historical encryption schemes and the one-time pad
2. stream ciphers and block ciphers
3. one-way functions and 2-party key exchange
4. digital signatures and public key encryption
5. design of cryptographic protocols with provable guarantees

Course participants are expected to deepen their understanding of the course material through exploring original sources and secondary literature on a weekly basis. References to pertinent literature or online resources will be provided in class.

Assessment Procedures

There will be five homework projects $\{H_1, H_2, H_3, H_4, H_5\}$, a midterm exam X_1 and a comprehensive final exam 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	Jan 19, 2013	15
H_2	Feb 5, 2013	15
H_3	Mar 14, 2013	15
H_4	Mar 28, 2013	15
H_5	Apr 11, 2013	15
X_1	Feb 19, 2013	25
X_2	Apr 25, 2013	30

Exams will be given in class. Take-home exam may involve a moderate amount of programming; if this is the case, you are free in choosing the programming language. Homework projects and take-home exams will be **assigned** in class at the date specified above and are **due 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 two lowest scores achieved in the items $\{H_1, H_2, H_3, H_4, H_5\}$ are dropped. The points from the remaining three items and of the two items $\{X_1, X_2\}$ are added, yielding a final score $0 \le P \le 100$.
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
≥ 50 – 53	D–
<50	F

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, and you document this, then you can make up the respective assignment.
Extra credit work is not possible.

Method of Instruction

The course is conducted in lecture/discussion style.

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 – LA 240 (954-236-1222), 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

Students are responsible for informing themselves about FAU's Code of Academic Integrity before performing any academic work—more detailed information is available at the URL *http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf*.
Scholastic dishonesty includes, but is not limited to, plagiarism and copying other's work during an exam. Any exam or written assignment for which you are caught cheating will be marked as a zero grade, and the incident will be reported in accordance with the Code of Academic Integrity.