1. General

Course information.

- Semester: Spring, 2017.
- Lecture Time: 05:30 p.m. – 06:50 p.m. Monday and Wednesday.
- Lecture Venue: FL404.
- Credit hours: 3 credits.
- Instructor: Shi Bai, SE230, `sbai@fau.edu`
- Website: `http://cosweb1.fau.edu/~sbai/teaching/2017/mad6478`

Office hours. Monday and Wednesday 4:00 – 5:00 p.m. and by appointment. Also, feel free to come to the office whenever time permits, questions and discussions are welcome.

Content. Cryptanalysis employs mathematical and algorithmic tools to evaluate the security level of cryptographic systems and protocols. The course explains standard cryptanalysis techniques used for analyzing and attacking different types of cryptographic schemes, focusing on aspects of public-key cryptography. The purpose of this course is to allow students to understand the mathematical and algorithmic principles underlying a wide variety of of cryptanalysis techniques. A tentative lecture plan includes:

- general background: security requirements and models;
- security of RSA, DH;
- basic algorithmic number theory;
- algorithms for integer factorization;
- algorithms for discrete logarithms;
- lattice cryptography and lattice reduction algorithms;
- side channel attacks (e.g., timing and power analysis);
- cryptanalysis of block ciphers;
- Additional topics may include: quantum algorithms.

There will be several modules for this course. We will start by discussing the security requirements and attack models that are being used in modern cryptosystems. A main focus of the course is to understand the computational hardness underlying certain cryptosystems such as RSA/DLP/lattice cryptography. We will be discussing mathematical algorithms for these computational assumptions – after completion of the module – you should be able to explain and apply typical algorithms used for factoring integers, computing discrete logarithms and understand algorithms for lattice reduction. In addition to mathematical analysis of the computational assumptions, we will also discuss side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation – 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.

Pre-requisites. The prerequisite is MAD 6477 (or MAD 5474). We assume general familiarity with cryptography. Some background on algebra and programming is certainly helpful, but not required. The course will be self contained; we shall develop all the machinery that we need.

Textbooks. The course will not follow a particular textbook, and necessary material will be distributed in class or on the course web site as needed. For some topics we will use journal and conference articles.

Supplementary reading. For additional reading the following books may be considered,

Gal12 Steven D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press 2012.

Jou09 Antoine Joux, *Algorithmic Cryptanalysis*, Chapman and Hall/CRC 2009.

CFA05 Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, Frederik Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography* , Chapman and Hall/CRC 2005.

CrP05 Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective*, Springer 2005 (2nd edition).

Wag02 Samuel S. Wagstaff, Jr., *Cryptanalysis of Number Theoretic Ciphers*, Chapman and Hall/CRC 2002.

KL14 Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, Chapman and Hall/CRC 2014.

2. Evaluation

The grade for the course will be determined by the following scheme:

Two assignments (40%), Project (60%).

Assignments. There will be two assignments for the course, each of which counts for 20% of the grade. Assignments should be clearly handwritten or printed on paper or sent by email in PDF formats. Late assignments will not be accepted and graded with 0 points.

Project. A research project will be given for each student, which counts for 60% of the class grade. The purpose is to develop students' understanding on the current state-of-the-art of the research in cryptanalysis. In the beginning of the semester, a list of research paper will be given. Each student must choose one item in the list and study the paper. Additional research paper (other than from the list) may be acceptable after discussion with the instructor but each paper must be relevant to the course content. The evaluation of the project consists of two components:

- A report (e.g. 5-10 pages) summarizing the main techniques of the research paper. The report counts for 30% of the total grade.
- An oral exam (45 minutes). The examiners will ask questions on your report; on your understanding of the technical contents of the research paper; and also relevant materials that cover the topics taught during the semester. The oral exam counts for 30% of the total grade.

The time of the oral exam will be during the exam week. The report should be submitted prior to the oral exam.

Grading scale. At the end of the semester, the following scale for FAU grade will be used.

%	92-100	87-91	84-86	81-83	78-80	75-77	72-74	69-71	66-68	63-65	60-62	0-59
Grade	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Graded assignment, and project report will be returned in class or can be picked up during office hours at the instructors office.

3. Course Policies

Students are expected to be familiar and comply with the standard university policies. In addition, the following policies on assignments should conformed.

Collaboration policy on assignments. Collaboration on the assignments is **permitted** for this course. If you do collaborate, your write-ups must be done independently and you must **acknowledge** your collaborators in your write-up. Failure to do so constitutes plagiarism.

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