FLORIDA ATLANTIC UNIVERSITY

Graduate Programs—NEW COURSE PROPOSAL

UGPC APPROVAL ________________
UFS APPROVAL ________________
SCNS SUBMITTAL ________________
CONFIRMED ____________________
BANNER POSTED ________________
ONLINE ______________________
MISC ________________________

DEPARTMENT NAME:
DEPARTMENT OF MATHEMATICAL SCIENCES

COLLEGE OF:
CHARLES E. SCHMIDT COLLEGE OF SCIENCE

RECOMMENDED COURSE IDENTIFICATION:

PREFIX MAD_____________ **COURSE NUMBER** 5474_________ **LAB CODE** (L or C) C____

(TO OBTAIN A COURSE NUMBER, CONTACT ERUDOLPH@FAU.EDU)

COMPLETE COURSE TITLE

INTRODUCTION TO CRYPTOLOGY AND INFORMATION SECURITY

EFFECTIVE DATE

(first term course will be offered)

____

CREDITS:
3

TEXTBOOK INFORMATION:
REQUIRED TEXT: J. KATZ AND Y. LINDELL: INTRODUCTION TO MODERN CRYPTOGRAPHY (CHAPMAN & HALL/CRC PRESS)
SUPPLEMENTARY TEXT: NONE

GRADING *(SELECT ONLY ONE GRADING OPTION)*: REGULAR _X____ PASS/FAIL ______ SATISFACTORY/UNSATISFACTORY ______

COURSE DESCRIPTION, NO MORE THAN 3 LINES:
CLASSICAL CIPHERS AND THEIR ANALYSIS; UNCONDITIONAL VS. COMPUTATIONAL SECURITY; BASIC CONSTRUCTIONS FOR STREAM CIPHERS; EXAMPLES AND MODES OF OPERATION OF BLOCK CIPHERS; CRYPTOGRAPHIC HASH FUNCTIONS; PUBLIC KEY ENCRYPTION WITH ELGAMAL AND RSA; DIGITAL SIGNATURE SCHEMES; DIFFIE-HELLMAN KEY EXCHANGE

PREREQUISITES W/MINIMUM GRADE:*

MAS 2103 MATRIX THEORY (MINIMUM GRADE C) AND

MAD 2502 INTRODUCTION TO COMPUTATIONAL MATHEMATICS (MINIMUM GRADE C)

COREQUISITES:

NONE

OTHER REGISTRATION CONTROLS (MAJOR, COLLEGE, LEVEL):

NONE

PREREQUISITES, COREQUISITES & REGISTRATION CONTROLS SHOWN ABOVE WILL BE ENFORCED FOR ALL COURSE SECTIONS.

****DEFAULT MINIMUM GRADE IS D-.***

MINIMUM QUALIFICATIONS NEEDED TO TEACH THIS COURSE:
ASSISTANT PROFESSOR

Other departments, colleges that might be affected by the new course must be consulted. List entities that have been consulted and attach written comments from each.
Department of Computer Science & Engineering

Rainer Steinwandt, rsteinwa@fau.edu, 561-297-3353
Faculty Contact, Email, Complete Phone Number

SIGNATURES

SUPPORTING MATERIALS

Approved by:	***Date:***	**Syllabus**—must include all details as shown in the UGPC Guidelines.
Department Chair: ______________________	______________	**Written Consent**—required from all departments affected.
College Curriculum Chair: ________________	______________	Go to: *http://graduate.fau.edu/gpc/* to download this form and guidelines to fill out the form.
College Dean: __________________________	______________	
UGPC Chair: ___________________________	______________	
Dean of the Graduate College: ______________	______________	

Email this form and syllabus to sfulks@fau.edu and *eqirjo@fau.edu* one week ***before*** the University Graduate Programs Committee meeting so that materials may be viewed on the UGPC website by committee members prior to the meeting.

Syllabus

Course Name

Introduction to Cryptology and Information Security

Course Number

MAD 5474

Section Number

N/A

Prerequisites

- MAS 2103 Matrix Theory (Minimum Grade C) and
- MAD 2502 Introduction to Computational Mathematics (Minimum Grade C)

Credit Hours

3

Instructor

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

Required Text

Introduction to Modern Cryptography by J. Katz and Y. Lindell, Chapman & Hall/CRC Press, 2007

Bibliography

- *Classical Introduction to Cryptography. Applications for Communications Security* by S. Vaudenay, Springer, 2006
- *Cryptography. Theory and Practice* by D.R. Stinson, Chapman & Hall/CRC, 2006
- *Foundations of Cryptography: Volume 1, Basic Tools* by O. Goldreich, Cambridge University Press, 2001
- *Foundations of Cryptography: Volume 2, Basic Applications* by O. Goldreich, Cambridge University Press, 2004
- *Handbook of Applied Cryptography* by A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, CRC Press, 2001
- *Introduction to Cryptography* by J.A. Buchmann, Springer, 2004
- *Practical Cryptography* by N. Ferguson and B. Schneier, Wiley Publishing, 2003

Course Objectives

The course explains standard techniques for analyzing and designing different types of cryptographic schemes. After completion of the course, you should be able to name and explain fundamental cryptographic tasks and basic attack techniques. You should be able to give examples of symmetric encryption algorithms and be able to explain how they work and in which way they are used. Similarly, you should be able to give examples and explain techniques used in public key encryption.

After completion of the course, you should have developed a clear understanding of the mathematical techniques underlying standard methods for factoring integers and computing discrete logarithms and their relevance for cryptanalysis.

Lecture Schedule

- Historical ciphers and their cryptanalysis (ca. 1 week)
- Perfect secrecy and the one time pad (ca. 1 week)
- Private-key encryption and pseudo-randomness (ca. 2 weeks)
- Message authentication codes and cryptographic hash functions (ca. 2 weeks)
- Block ciphers (ca. 2 week)
- Primes, factoring and RSA (ca. 2 weeks)
- Discrete logarithms, Diffie-Hellman assumption and ElGamal (ca. 2 weeks)
- Security against chosen-ciphertext attacks (ca. 1 week)
- Digital signature schemes (ca. 2 weeks)

Assessment Procedure and Grading

There will be graded homework assignments accounting for 40% of your cumulative performance, a midterm exam $X_{1,}$ accounting for 30% of your cumulative performance, and a final exam X_2 that accounts for 30% of your cumulative performance. Your overall grade in the course is derived from your cumulative performance according to the following table.

Cumulative Performance	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. Assignments may require the use of a computer and programming. Unless otherwise specified, 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 – 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 bet 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 the Honor Code standards before performing any academic work—more detailed information is available at the URL *http://www.fau.edu/regulations/chapter4/4.001_Honor_Code.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 Honor Code regulations.

Dr. Rainer Steinwandt, Professor
Department of Mathematical Sciences
Florida Atlantic University
777 Glades Road
Boca Raton, FL 33431
tel: 561.297.3353
fax: 561.297.2436
rsteinwa@fau.edu

Requirements in Proposed Graduate Course MAD 5474 vs. Undergradute Course CIS 4362

The proposed graduate course *Introduction to Cryptology and Information Security* is expected to be regularly collocated with the undergraduate course CIS 4362 on the same subject. Out of this reason already, existing FAU resources will be sufficient for offering the newly proposed course, and no additional support is requested.

Participants of MAD 5474 are expected to develop a more thorough understanding of design details of cryptographic protocols as is expected from participants of CIS 4362. To ensure this, homework projects and exams for MAD 5474 contain different and/or additional problems than those of the undergraduate course variant. Typically, an additional problem for the graduate course will require a student to identify a solution for a protocol weakness that has been identified in a part of an assignment that is shared with CIS 4362, or a participant of MAD 5474 will be required to prove a result, where for an undergraduate student the ability to apply the correct approach is already considered as sufficient. The Modern Algebra prerequisite of the course is to ensure the mathematical maturity of students to master the technical machinery that is needed for solving the problems not to be solved by CIS 4362 participants.

Similarly, if a homework project involves the implementation of an algorithm, in MAD 5474 efficiency requirements are to be taken into account properly, whereas for the undergraduate course correctness of a solution and the ability to work with smaller problem parameters may suffice already. Finally, for assignments in the graduate course it is expected that references to non-textbook material can be given (like a FIPS Publication issued by NIST), and that the student can use such a document to extract the relevant information for answering a homework problem specific to the newly proposed course MAD 5474.