FLORIDA ATLANTIC UNIVERSITY™

Graduate Programs—COURSE CHANGE REQUEST[1]

UGPC APPROVAL _____
UFS APPROVAL _____
SCNS SUBMITTAL _____
CONFIRMED _____
BANNER POSTED _____
CATALOG _____

DEPARTMENT MATHEMATICAL SCIENCES	COLLEGE CHARLES E. SCHMIDT COLLEGE OF SCIENCE
COURSE PREFIX AND NUMBER MAD 6478	CURRENT COURSE TITLE Cryptanalysis
CHANGE(S) ARE TO BE EFFECTIVE (LIST TERM) SPRING 2017	____ TERMINATE COURSE (LIST FINAL ACTIVE TERM)
CHANGE TITLE TO: CHANGE PREFIX FROM: TO: CHANGE COURSE NO. FROM: TO: CHANGE CREDITS[2] FROM: TO: CHANGE GRADING FROM: TO: CHANGE DESCRIPTION TO: Fundamental techniques to analyze cryptographic systems are introduced. Linear and differential cryptanalysis are explained, birthday attacks are analyzed, algorithms to factor integers and compute discrete logarithms are discussed, side-channel attacks are described.	CHANGE PREREQUISITES/MINIMUM GRADES TO*: (MAD 6477 WITH A GRADE OF "C" OR HIGHER) OR (MAD 5474 WITH A GRADE OF "C" OR HIGHER) (ORIGINAL PREREQUISITES: MAD 6477) CHANGE COREQUISITES TO*: CHANGE REGISTRATION CONTROLS TO: *Please list both existing and new pre/corequisites, specify AND or OR, and include minimum passing grade.
Faculty contact, email and complete phone number: Rainer Steinwandt, rsteinwa@fau.edu , 561-297-3353	**Attach syllabus for ANY changes to current course information.**
Should the requested change(s) cause this course to overlap any other FAU courses, please list them here:	Please consult and list departments that might be affected by the change(s) and attach comments.[3] Department of Computer & Electrical Engineering and Computer Science

Approved by:	*Date:*
Department Chair:	10/13/15
College Curriculum Chair:	11/15/15
College Dean:	11/15/15
UGPC Chair: Wm R McDaniel	12-9-15
Graduate College Dean:	12-11-15
UFS President:	
Provost:	

1. **Syllabus** must be attached; see guidelines for requirements: *www.fau.edu/provost/files/course syllabus.2011.pdf*

2. Review **Provost Memorandum: Definition of a Credit Hour** *www.fau.edu/provost/files/Definition_Credit_Hour_Memo_2012.pdf*

3. **Consent** from affected departments (attach if applicable)

Email this form and syllabus to *UGPC@fau.edu* **one week before** the University Graduate Programs Committee meeting.

Syllabus

1. COURSE TITLE	COURSE NUMBER	CREDIT HOURS
Cryptanalysis	MAD 6478	3

2. COURSE PREREQUISITES
(MAD 6477 Cryptography with a grade of "C" or higher) or
(MAD 5474 Introduction to Cryptology and Information Security with a grade of "C" or higher)

3. COURSE LOGISTICS

a. Spring 2017.
b. Taught in lecture-discussion style in-person (not online).
c. Course location is specified in the FAU course schedule.

4. INSTRUCTOR CONTACT INFORMATION
Rainer Steinwandt, Office SE 234A
Phone: (561) 297-3353, fax (561) 297-2436
E-mail address: rsteinwa@fau.edu
Office hours: Monday and Wednesday 9:30am–11:30am

5. TA CONTACT INFORMATION
N/A

6. COURSE DESCRIPTION
Fundamental techniques to analyze cryptographic systems are introduced. Linear and differential cryptanalysis are explained, birthday attacks are analyzed, algorithms to factor integers and compute discrete logarithms are discussed, side-channel attacks are described.

7. COURSE OBJECTIVES
Standard techniques to analyze different types of cryptographic schemes are explained. After completion of the course you should know common attacks against symmetric and asymmetric encryption schemes, and you should be able to characterize standard requirements for cryptographic hash functions and digital signatures schemes. You should also be able to judge the potential of elementary side-channel and fault induction attacks, e.g., based on the use of timing information, power consumption of a device, or through the induction of faults. Finally, you should be able to provide examples of protocol-level attacks against cryptographic protocols.

8. COURSE EVALUATION METHOD
There will be three homework projects $\{H_1, H_2, H_3\}$, each having a maximum score of 20 points. Homework project H_1 will be assigned in the 3rd week of classes, homework project H_2 will be assigned in the 7th week of classes, and homework project H_2 will be assigned in the 11th week of classes. The exact assignment due date will be specified on each assignment. Graded homework projects will be returned in class or can be picked up during office hours in the instructor's office.
In addition, there is a cumulative final exam, which is scheduled in accordance with FAU's final exam schedule. The maximum score for the final exam is 40 points.

9. COURSE GRADING SCALE
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 and the final exam are added, yielding a final number of points $0 \le P \le 100$.
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*

10. Policy on makeup tests, late work, and incompletes

If you cannot complete an assignment in due time to a relevant and documented reason, you can make up the respective assignment. Extra credit work is not possible.

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.

11. Special course requirements

N/A

12. Classroom etiquette policys

N/A

13. Disability policy statement

In compliance with the Americans with Disabilities Act (ADA), 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 Raton - SU 133 (561-297-3880), in Davie - MOD I (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.

14. Code of Academic Integrity policy statement

Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty, including cheating and plagiarism, 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 http://www.fau.edu/ctl/4.001_Code_of_Academic_Integrity.pdf .

15. Required texts/readings

Most reading assignments will be based on the following book, subsequently referred to as [KaLi15].

Jonathan Katz and Yehuda Lindell: *Introduction to Modern Cryptography*, second edition, Chapman & Hall/CRC Cryptography and Network Security Series, Taylor & Francis Group, 2015.

16. SUPPLEMENTARY READINGS

The following references can supplement the material covered in class.

- Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone: *Handbook of Applied Cryptography*, Discrete Mathematics and Its Applications Series, CRC Press, Taylor & Francis Group, 1996.
- Christof Paar, Jan Pelzl, and Bart Preneel: *Understanding Cryptography. A Textbook for Students and Practitioners*, Springer-Verlag, 2010.

17. COURSE TOPICAL OUTLINE

The following topics are to be covered. The exact duration per topic will vary in dependence on prior experience of the class participants, but a typical duration per topic is one week.

1) Cryptanalysis of historical ciphers and review of modern cryptographic principles – reading assignment: Sec. 1 in [KaLi15]

2) Basic attack models for encryption schemes such as IND-CPA and IND-CCA – reading assignment: Sec. 3.2, 3.4, 3.7 in [KaLi15]

3) Review of hash functions, generic attacks on them such as birthday attacks, time/space tradeoffs – reading assignment: Sec. 5.1, 5.4, Appendix A.4 in [KaLi15]

4) Review of block ciphers – reading assignment: Sec. 6.2.1 – 6.2.5 in [KaLi15]

5) Linear and differential cryptanalysis – reading assignment: Sec. 6.2.6 in [KaLi15].

6) Number-theoretic foundations – reading assignment: Sec. 8.1, 8.3 in [KaLi15].

7) Introduction to elliptic curves– reading assignment: Sec. 8.3.4 in [KaLi15]

8) Review of RSA, algorithms for factoring integers such as Pollard's $p-1$ algorithm, ECM, and the quadratic sieve – reading assignment: Sec. 9.1 in [KaLi15]

9) Review of Diffie-Hellman key exchange, algorithms for computing discrete logarithms such as the baby-step/giant-step algorithm and index calculus– reading assignment: Sec. 9.2 in [KaLi15]

10) Key management – reading assignment: Sec. 10 in [KaLi15]

11) Security goals for digital signatures – reading assignment: Sec. 12.1 – 12.4 in [KaLi15]

12) Verifiable secret sharing – reading assignment: Sec. 13.3 in [KaLi15]

13) Side-channel attacks such as timing attacks, SPA, and DPA – reading assignment: François-Xavier Standaert: *Introduction to Side-Channel Attacks* (Part of Secure Integrated Circuits and Systems, Integrated Circuits and Systems, pp. 27–42, Springer, 2010).

14) Fault attacks such as the Bellcore attack– reading assignment: Dan Boneh, Richard A. DeMillo and Richard Lipton: *On the Importance of Eliminating Errors in Cryptographic Computations*, J. of Cryptology 14(2): 101–120, 2001.