Department of Computer & Electrical Engineering and Computer Science
Florida Atlantic University
Course Syllabus

1. Course title/number, number of credit hours	
Practical Aspects of Modern Cryptography CIS 5371	3 credit hours
2. Course prerequisites, corequisites, and where the course fits in the program of study	
Prerequisites: Graduate Status Level or MAD2104 and COP3014.	
3. Course logistics	
Term: Fall 2017 *Class location and time*: TBD	
4. Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	Mehrdad Nojoumian EE96, Room 530 TBD 561.297.3411 mnojoumian@fau.edu
5. TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	
6. Course description	
Topics to be covered: (A) Mathematical background, algorithmic number theory, classical crypto, implementation aspects of private-key crypto, implementation aspects of public-key crypto, and (b) Advanced topics on crypto such as crypto primitives, rational crypto, secure multiparty computation, hash functions, digital signatures, and privacy-preserving protocols.	
7. Course objectives/student learning outcomes/program outcomes	
Course objectives	This course enables the students to review basic mathematical aspects of applied cryptography as well as fundamental concepts of cryptographic algorithms. Furthermore, it enables the students to utilize these techniques in computing systems through programming languages.
Student learning outcomes & relationship to ABET a-k objectives	

Department of Computer & Electrical Engineering and Computer Science
Florida Atlantic University
Course Syllabus

8. Course evaluation method

Five Assignments (each 4%) - 20% Project - 30% Project Presentation - 20% Final Exam - 30%	**Project:** students are supposed to select one of the following options: (a) implement a cryptographic scheme with all modules, or (b) prepare a technical article on modern cryptographic protocols, e.g., homomorphic encryption/multiparty computation.

9. Course grading scale

Grading Scale:
90 and above: "A", 87-89: "A-", 83-86: "B+", 80-82: "B", 77-79 : "B-", 73-76: "C+", 70-72: "C", 67-69: "C-", 63-66: "D+", 60-62: "D", 51-59: "D-", 50 and below: "F."

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

All assignments are due at 11:00 am on the due date. Late assignments will lose 10% of the total points for each day they are late and they will not be accepted after three days. However, appropriate accommodations will be made for students having a valid medical excuse. Unless there exists an evidence of medical or emergency situation, incomplete grades will not be given. Plagiarism will not be tolerated. Any copying and pasting without attribution and a reference will be considered plagiarism.

11. Special course requirements

N/A

12. Classroom etiquette policy

University policy requires that in order to enhance and maintain a productive atmosphere for education, personal communication devices, such as cellular phones and laptops, are to be disabled in class sessions.

13. Disability policy statement

In compliance with the Americans with Disabilities Act, students who require special accommodations due to a disability to properly execute coursework must register with the FAU Students Accessibility Services (SAS) located in Boca Raton, Davie, and Jupiter campuses and follow all SAS procedures http://www.fau.edu/sas.

14. 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 unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and place high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. See University Regulation 4.001 at http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf

15. Required texts/reading

Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC, 1997.
ISBN: 0-8493-8523-7

Department of Computer & Electrical Engineering and Computer Science
Florida Atlantic University
Course Syllabus

16. Supplementary/recommended readings

Cryptography Theory and Practice (3rd edition), Stinson, Chapman & Hall/CRC, 2006.
ISBN: 978-1-58488-508-5
Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC, 2015.
ISBN: 978-1-4665-7026-9

17. Course topical outline, including dates for exams/quizzes, papers, completion of reading

Weekly Schedule	Topics
Week 01	Introduction: Terminologies and Security Models Preliminary Materials: Modular Arithmetic and Integer Representations
Week 02	Preliminary Materials: Prime Numbers, GCD and LCM Preliminary Materials: Euclidean Algorithm and Extended Euclidean Alg.
Week 03	Preliminary Materials: Congruence, Primitive Root, Discrete Log and RNG Preliminary Materials: Functions, Injection, Surjection and Bijection
Week 04: **Assig-01**	From Classical to Modern Cryptography Stream Ciphers
Week 05	Software Implementation of Block Cipher: DES - Data Encryption Standard
Week 06: **Assig-02**	Software Implementation of Block Cipher: AES - Advanced Encryption Standard
Week 07	Implementation of RSA Using Large Integers & Its Security Proof: Modular Exponentiations, Primality Test and Their Complexities
Week 08: **Assig-03**	Implementations of ElGamal and Rabin Algorithms Using Large Integers Their Security Proofs and Applications
Week 09	Randomized Algorithms: Las Vegas and Monte Carlo Algorithms Probabilistic Public-Key Encryption: Blum-Goldwasser
Week 10: **Assig-04**	Secret Sharing Schemes Rational Cryptography
Week 11	Secure Multiparty Computation Cryptographic Hash Functions
Week 12: **Assig-05**	Hash Functions Based on Block Ciphers Hash Functions Based on Modular Arithmetic
Week 13	Digital Signatures Digital Signatures With Message Recovery
Week 14	Privacy-Preserving Protocols Sealed-Bid Auctions and Secure Mechanism Design
Week 15	Project Submission and Project Presentation
	Final Exam