Department of Mathematical Sciences
Florida Atlantic University
Course Syllabus

Course title/number, number of credit hours	
Mathematics for Cryptography/MAS 4218, 3 cr	
Course prerequisite	
(MAD 2104 Discrete Mathematics with a minimum grade of C) AND (MAS 2103 Matrix Theory with a minimum grade of C)	
Course logistics	
Term: Fall 2020/ This is a classroom lecture *Class location and time:* TBA	
Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	Koray Karabina SE 266 TBA 561-297-0809 kkarabina@fau.edu
TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	TBA
Course description	
This course will introduce students to the mathematical foundations of cryptography. This includes probability theory, modular arithmetic, selected topics from number theory, coding theory, and lattices. In this course, students will learn how mathematics is used in the construction and analysis of cryptographic schemes with some applications in modern cryptography.	
Course objectives/student learning outcomes	
Course objectives	**Objectives:** • Learn how mathematics is used in the design and analysis of cryptographic schemes. • Learn the underlying mathematical principals of modern cryptography. ***Outcomes:*** • Develop ability to use mathematical tools in the design and analysis of cryptographic schemes. • Develop ability to understand and analyze advanced cryptographic algorithms and their applications.
Course evaluation method	
• 5 Homework Assginments (Week 2, Week 4, Week 8, Week 10, Week 12) The lowest two scores are dropped, each of the remaining three is worth 15% of the grade.	

- Mid-term exam (Week 6): 20% of the grade.
- Final exam: 35% of the grade.

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."

Policy on makeup tests, late work, and incompletes

No late work is accepted unless special permission from the instructor. A grade of *Incomplete* will only be assigned in accordance with the University catalog.

Attendance policy statement

Students are expected to attend all of their scheduled University classes and to satisfy all academic objectives as outlined by the instructor. The effect of absences upon grades is determined by the instructor, and the University reserves the right to deal at any time with individual cases of non-attendance.
Students are responsible for arranging to make up work missed because of legitimate class absence, such as illness, family emergencies, military obligation, court-imposed legal obligations or participation in University-approved activities. Examples of University-approved reasons for absences include participating on an athletic or scholastic team, musical and theatrical performances and debate activities. It is the student's responsibility to give the instructor notice prior to any anticipated absences and within a reasonable amount of time after an unanticipated absence, ordinarily by the next scheduled class meeting. Instructors must allow each student who is absent for a University-approved reason the opportunity to make up work missed without any reduction in the student's final course grade as a direct result of such absence.

Disability policy statement

In compliance with the Americans with Disabilities Act Amendments Act (ADAAA), students who require reasonable accommodations due to a disability to properly execute coursework must register with Student Accessibility Services (SAS) and follow all SAS procedures. SAS has offices across three of FAU's campuses – Boca Raton, Davie and Jupiter – however disability services are available for students on all campuses. For more information, please visit the SAS website at www.fau.edu/sas/.

Counseling and Psychological Services (CAPS) Center

Life as a university student can be challenging physically, mentally and emotionally. Students who find stress negatively affecting their ability to achieve academic or personal goals may wish to consider utilizing FAU's Counseling and Psychological Services (CAPS) Center. CAPS provides FAU students a range of services – individual counseling, support meetings, and psychiatric services, to name a few – offered to help improve and maintain emotional well-being. For more information, go to http://www.fau.edu/counseling/

Code of Academic Integrity policy statement

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 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.

Required texts/reading

Purchasing a textbook is *not* required, and the material and assignments presented in class will be self-contained. However, the presentation will largely follow the order of presentation in the book by Hoffstein et al. listed in the supplementary/recommended readings section.

Supplementary/recommended readings

J. Hoffstein, J. Pipher, and J. H. Silverman: *An Introduction to Mathematical Cryptography*
Springer, 2014
ISBN 978-1-4939-1710-5

Subsequently this book is referenced as [HPS14].

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

Weekly Schedule	**Topics**
Week 01	Introduction to Cryptography and Modular Arithmetic (Ch. 1.1 – 1.3 of [HPS14])
Week 02	Prime Numbers, Factorization, Finite Fields; Homework 1 (Ch. 1.4 – 1.6 of [HPS14])
Week 03	Discrete Logarithm Problem (DLP), DLP-Solvers, Cryptographic Applications of the DLP (Ch. 2.1 – 2.7, 2.9 of [HPS14])
Week 04	RSA and Primality Testing; Homework 2 (Ch. 3.1 – 3.4 of [HPS14])
Week 05	Integer Factorization (Ch. 3.5 – 3.8)
Week 06	Combinatorics and Probability; Midterm (Ch. 4.1 – 4.5 of [HPS14])
Week 07	Elliptic Curves over Finite Fields (Ch. 5.1 – 5.2 of [HPS14])
Week 08	Elliptic Curve Cryptography; Homework 3 (Ch. 5.1 – 5.4 of [HPS14])
Week 09	Introduction to Lattices (Ch. 6.1 – 6.4 of [HPS14])

Week 10	Lattice-Based Cryptography; Homework 4 (Ch. 6.7 – 6.10)
Week 11	Lattice Reduction (Ch. 6.11 – 6.13 [HPS14])
Week 12	Digital Signatures; Homework 5 (Ch. 7.1 – 7.4 of [HPS14])
Week 13	Coding Theory Linear Codes and Decoding Algorithms (Supplementary Material)
Week 14	Code Based Cryptography McEliece Cryptosystem (Supplementary Material)
Week 15	Review; Final exam