**Florida Atlantic University**

**Department of Mathematical Sciences**

**Introduction to Cryptography and its Applications
MAD 2470**

**Spring 2018**

**3 Credit Hours**

**Instructor:** Dr. Koray Karabina

**Office Location:** SE 266

**Office Hours:** TBA

**Contact Phone Number:** 561-297-0809

**Email:** kkarabina@fau.edu

**Course Prerequisites:** Instructor’s permission

**Time Commitment per Credit Hour:** This course has 3 credit hours. For traditionally delivered courses, not less than one (1) hour of classroom or direct faculty instruction each week for fifteen (15) weeks per Fall or Spring semester, and a minimum of two (2) hours of out-of-class student work for each credit hour. Equivalent time and effort is required for Summer Semesters, which may be offered over a shortened time frame. Fully Online courses, hybrid, shortened, intensive format courses, and other non-traditional modes of delivery will demonstrate equivalent time and effort.

**Course Description/Introduction**

Cryptography is a method for protecting information against unauthorized parties also known as attackers. Classical cryptography dates back to ancient times (2000 BC) and has naturally evolved from art to science. In our modern world, cryptography lies at the intersection of mathematics, computer science, and engineering. Objectives of this course are twofold. First, students will master some mathematical techniques used in the design and analysis of cryptographic algorithms. We will cover a wide range of examples including some historical ciphers (e.g. Ceasar cipher) and modern ctyptographic algorithms (e.g. DES, AES, RSA). Second, students will gain hands-on experience in real life applications (e.g. password based authentication, online banking) and implementation of cryptographic algorithms.

By the end of the course, it is expected that students will have in-depth understanding of modern cryptographic algorithms, their real-life applications and implementation. More technical course content is summarized below.

Course content: Cryptographic applications; classical ciphers and their cryptanalysis; symmetric key cryptography; block ciphers; stream ciphers; cryptographic hash functions; message authentication codes; public key cryptography; encryption and digital signature schemes (RSA and ElGamal); key agreement protocols (Diffie-Hellman); real life deployments and applications.

**Course Objectives**

1. Define the security of fundamental cryptographic primitives and systems
2. Analyze security of symmetric and public key schemes, hash functions, message authentication codes and cryptographic protocols
3. Define and apply generic cryptanalysis methods including brute force, frequency analysis, meet-in-the-middle attacks
4. Examine symmetric key and public key schemes: encryption functions, hash functions, message authentication codes, signature schemes. Key establishment protocols.
5. Identify applications, real-life deployment, and learn about the history standardization of cryptographic constructions
6. Develop mathematical and programming skills for implementing cryptographic algorithms and for analyzing their security
7. Master basic number theoretical, algorithmic, probabilistic, and statistical notions and apply this knowledge in cryptanalysis

**Course Delivery Mode**

This course is accessible through FAU’s learning management system—Canvas. You must log into Canvas with your FAU ID and Password to access the materials and assignments in this course. If you do not know your FAU ID or Password click the following link for help. [Link to Office of Information Technology Help](http://www.fau.edu/oit/accounts/index.php).

**Required Text and Materials**

Understanding Cryptography: A Textbook for Students and Practitioners
Url: http://www.crypto-textbook.com/
ISBN-13: 978-3642041006
ISBN-10: 3642041000
[Christof Paar](https://www.amazon.com/Christof-Paar/e/B0034NXPFW/ref%3Ddp_byline_cont_book_1) and [Jan Pelzl](https://www.amazon.com/Jan-Pelzl/e/B0045AGXLQ/ref%3Ddp_byline_cont_book_2)

**Course Assessments, Assignments, Grading Policy, and Course Policies**

**Assignments: A Total of 50 points**

There will be a total of 11 assignments throughout the term. Questions in these assignments will be testing students’ knowledge on both theory and applications. Assignments are worth a total of 50 points. Assignments may not be weighted equally.

No late submissions will be accepted and make-ups are not allowed. Your instructor will mark all written assignments. You must show all of your work to receive full mark. Your solutions must be legible and well organized.

**Exams: A total of 50 points**

There will be a total of 2 midterm exams and 1 final exam. Each midterm exam is worth 30 points, and the final exam is worth 20 points.

Your instructor will mark all exams. You must show all of your work to receive full mark. Your solutions must be legible and well organized.

**Grading and Scale**

There are maximum 100 points to collect in this course. Total number of points collected by a student will be converted to a final letter grade according to the following catalogue:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TotalPoints | 87-100 | 83-86 | 77-82 | 73-76 | 70-72 | 67-69 | 63-66 | 60-62 | 57-59 | 53-56 | 50-52 | <50 |
| Grade | A | A- | B+ | B | B- | C+ | C | C- | D+ | D | D- | F |

**Late Assignments and Quizzes Policy**

Late assignments will not be accepted except in very special circumstances.

**Make-up Policy for Assignments and Quizzes:**

You will have plenty of time to work on the assignment problems and so **no late submissions will be accepted and no make-up for assignments.**

Make-up exams will be given only under extraordinary circumstances such as such as illness, family emergencies, military obligation, court-imposed legal obligations, or participation in university-approved activities – See FAU website for a list of university-approved activities. If you miss a quiz, you must provide a written, verifiable excuse, if possible in advance of the scheduled exam. Doctor notes, letters, emails from immediate family members are not accepted as proof of absence from any quizzes. Approval for a make-up quiz must be obtained from your instructor.

**Incomplete Grade Policy**

The University policy states that a student who is passing a course, but has not completed all work due to exceptional circumstances, may, with consent of the instructor, temporarily receive a grade of incomplete (“I”). The assignment of the “I” grade is at the discretion of the instructor, but is allowed only if the student is passing the course.

**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](http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf).

[Plagiarism](http://libguides.fau.edu/c.php?g=325629&p=2352760) is unacceptable in the University community. Academic work that is submitted by students is assumed to be the result of their own thought, research, or self-expression. When students borrow ideas, wording, or organization from another source, they are expected to acknowledge that fact in an appropriate manner. Plagiarism is the deliberate use and appropriation of another's work without identifying the source and trying to pass off such work as one’s own. Any student who fails to give full credit for ideas or materials taken from another has plagiarized. This includes all discussion board posts, journal entries, wikis, and other written and oral presentation assignments. If in doubt, cite your source!

 **Netiquette and Classroom Etiquette Policy**

**Netiquette**

Due to the casual communication common in the online environment, students are sometimes tempted to relax their grammar, spelling, and/or professionalism. Please remember that you are adult students and professionals—your communication should be appropriate.

For more in-depth information, please see the FAU statement on Netiquette at:

[Link to Netiquette policy](http://www.fau.edu/oit/student/netiquette.php)

**Classroom Etiquette/Disruptive Behavior Policy Statement**

Disruptive behavior is defined in the FAU Student Code of Conduct as *“... activities which interfere with the educational mission within classroom.”* Students who behave in the face-to-face and/or virtual classroom such that the educational experiences of other students and/or the instructor’s course objectives are disrupted are subject to disciplinary action. Such behavior impedes students’ ability to learn or an instructor’s ability to teach. Disruptive behavior may include, but is not limited to: non-approved use of electronic devices (including cellular telephones); cursing or shouting at others in such a way as to be disruptive; or, other violations of an instructor’s expectations for classroom conduct.

For more information, please see the FAU Office of Student Conduct:

[Link to Student Conduct](http://www.fau.edu/studentconduct/) Policy

**Communication Policy**

**Expectations for Students**

* Announcements
	+ You are responsible for reading all announcements posted by the instructor. Check the course announcements each time you log in.
* Email
* You are responsible for reading all of your course email and responding in a timely manner.
* Course-Related Questions
	+ Post course-related questions to the FAQ discussion board. This allows other participants with the same question to benefit from the responses. Also, make sure you review this forum prior to posting a question; it may have already been asked and answered in previous posts.

**Instructor’s Plan for Classroom Response Time & Feedback**

* Email Policy
	+ Except for Saturdays, Sundays, and holidays, instructor typically, will respond to messages within 48 hours. Such messages should only be used to communicate personal or confidential matters; otherwise, please use the FAQ discussion board within the course.
* Assignment Feedback Policy
	+ Feedback will be provided on submitted assignments within one week of the submission date. Some assignments may require a longer review period, which will be communicated to students by the instructor.
* Course-Related Questions
	+ Except Saturdays, Sundays, and holidays, questions will, generally, be answered by instructors within 48 hours.

**Support Services and Online Resources**

|  |  |
| --- | --- |
| Office of Information Technology Online Help Desk:  | [Link to FAU Help Desk](http://helpdesk.fau.edu/) |
| FAU Libraries:  | [Link to FAU Library](http://www.fau.edu/library/) |
| Center for Learning and Student Success:  | [Link to FAU Center for Learning](http://www.fau.edu/class) |
| University Center for Excellence in Writing:  | [Link to FAU Excellence in Writing](http://www.fau.edu/UCEW)  |
| Math Learning Center:  | [Link to FAU Math Center](http://www.math.fau.edu/MLC) |
| Office of Undergraduate Research and Inquiry:  | [Link to FAU Undergraduate Research](http://www.fau.edu/ouri) |
| Student Accessibility Services: | [Link to FAU Student Accessibility Services](http://www.fau.edu/sas)  |
| Office of International Programs and Study Abroad:  | [Link to FAU International Programs](http://www.fau.edu/goabroad)  |
| Freshman Academic Advising Services:  | [Link to FAU Freshman Advising](http://www.fau.edu/freshmanadvising) |

**Faculty Rights and Responsibilities**

Florida Atlantic University respects the rights of instructors to teach and students to learn. Maintenance of these rights requires classroom conditions which do not impede their exercise. To ensure these rights, faculty members have the prerogative:

* To establish and implement academic standards.
* To establish and enforce reasonable behavior standards in each class.
* To refer disciplinary action to those students whose behavior may be judged to be disruptive under the *Student Code of Conduct*.

Instructor reserves the right to adjust this syllabus as necessary.

**Selected University and College Policies**

**Accessibility Policy Statement**

In compliance with the Americans with Disabilities Act (ADA), students who require special accommodations to properly execute coursework due to a disability, must register with Student Accessibility Services (SAS) located in the Boca Raton, Davie, and Jupiter campuses and follow all SAS procedures. For additional information, please see: [Link to Student Accessibility Services](http://www.fau.edu/sas).

Questions relating to academic accommodations for students with disabilities are to be directed to Students Accessibility Services, Boca Raton campus, Room 133, (561) 297-3880, TDD (561) 297-0358.

**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 3 without any reduction in the student’s final course grade as a direct result of such absence.

**Grade Appeal Process**

A student may request a review of the final course grade when s/he believes that one of the following conditions apply:

* There was a computational or recording error in the grading.
* Non-academic criteria were applied in the grading process.
* There was a gross violation of the instructor’s own grading system.
* Procedures for a grade appeal may be found in [Chapter 4 of the University Regulations](http://www.fau.edu/regulations/chapter4/index.php).

**Religious Accommodation Policy Statement**

In accordance with rules of the Florida Board of Education and Florida law, students have the right to reasonable accommodations from the University in order to observe religious practices and beliefs with regard to admissions, registration, class attendance, and the scheduling of examinations and work assignments.  For further information, please see [Academic Policies and Regulations](http://www.fau.edu/academic/registrar/FAUcatalog/academics.php).

**University Approved Absence Policy Statement**

In accordance with rules of the Florida Atlantic University, students have the right to reasonable accommodations to participate in University approved activities, including athletic or scholastics teams, musical and theatrical performances and debate activities. It is the student’s responsibility to notify the instructor at least one week prior to missing any course assignment.

**Drops/Withdrawals**

Students are responsible for completing the process of dropping or withdrawing from a course. Please click on the following link for more information on dropping and/or withdrawing from a course. [Link to FAU Registrar Office](http://www.fau.edu/registrar/registration/faqs.php)

**Course Schedule**

|  |  |  |
| --- | --- | --- |
| Content | Assignments | Exams |
| Week 1 – Overview and historical ciphers |  |  |
| Week 2 – Symmetric key cryptography |  |  |
| Week 3 – Cryptanalysis | Ch 1: 1.1--1.6 |  |
| Week 4 – Stream ciphers | Ch 2: 2.1--2.6 |  |
| Week 5 – DES | Ch 3: 3.1--3.6  | Exam 1 |
| Week 6 – AES | Ch 4: 4.1-- 4.6 |  |
| Week 7 – Block ciphers | Ch 5: 5.1--5.5 |  |
| Week 8 – Public key cryptography | Ch 6: 6.1--6.6 |  |
| Week 9 – Modular arithmetic |  |  |
| Week 10 – RSA | Ch 7: 7.1--7.7 | Exam 2 |
| Week 11 – ElGamal | Ch 8: 8.1--8.5 |  |
| Week 12 – Hash functions | Ch 11: 11.1--11.5 |  |
| Week 13 – Message authentication codes | Ch 12: 12.1--12.5 |  |
| Week 14 – Digital signatures | Ch 10: 10.1--10.5 |  |
| Week 15 – Applications |  | Final Exam |