

 FLORIDA ATLANTIC UNIVERSITY	COURSE CHANGE REQUEST Graduate Programs		UGPC Approval _____ UFS Approval _____ SCNS Submittal _____ Confirmed _____ Banner _____ Catalog _____
	Department CEECS College Engineering and Computer Science		
Current Course Prefix and Number CIS 5371	Current Course Title Practical Aspects of Modern Cryptography		
Syllabus must be attached for ANY changes to current course details. See Guidelines . Please consult and list departments that may be affected by the changes; attach documentation.			
Change title to: Change prefix From: _____ To: _____ Change course number From: _____ To: _____ Change credits* From: _____ To: _____ Change grading From: _____ To: _____ Academic Service Learning (ASL) ** Add <input type="checkbox"/> Remove <input type="checkbox"/>		Change description to: Change prerequisites/minimum grades to: Graduate standing Change corequisites to: Change registration controls to:	
* Review Provost Memorandum ** Academic Service Learning statement must be indicated in syllabus and approval attached to this form.		Please list existing and new pre/corequisites, specify AND or OR and include minimum passing grade.	
Effective Term/Year for Changes: Spring 2021	Terminate course? Effective Term/Year for Termination:		
Faculty Contact/Email/Phone Hanqi Zhuang/zuang@fau.edu/ 297-3413			
Approved by Hanqi Zhuang Department Chair _____ College Curriculum Chair Francisco Presuel-Moreno College Dean McCardei UGPC Chair _____ UGC Chair _____ Graduate College Dean _____ UFS President _____ Provost _____		Date _____ _____ 10/25/2020 _____ _____ _____ _____	
<small>Digitally signed by Hanqi Zhuang Date: 2020.10.21 15:43:31 -04'00'</small>		<small>Digitally signed by Francisco Presuel-Moreno DN: cn=Francisco Presuel-Moreno, o=Florida Atlantic University, ou=Ocean and Mechanical Engineering, email=fpresuel@fau.edu, c=US Date: 2020.10.22 12:36:44 -04'00'</small>	
<small>Digitally signed by Michael Cardei DN: cn=Michael Cardei, o=Florida Atlantic University, ou= email=mcardei@fau.edu, c=US Date: 2020.10.23 19:39:22 -04'00'</small>			

Email this form and syllabus to UGPC@fau.edu 10 days before the UGPC meeting.

**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 standing		
3. Course logistics		
Term: Class location and time:		
4. Instructor contact information		
Instructor's name Office address Office Hours Contact telephone number Email address		
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- and 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.
8. Course evaluation method		
Five Assignments (each 4%) -	20%	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.
Project -	30%	
Project Presentation -	20%	
Final Exam -	30%	
9. Course grading scale		

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

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 11:59 pm 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. Makeup tests are given only if there is solid evidence of a medical or otherwise serious emergency that prevented the student of participating in the exam. Final exam will not have a makeup test under any circumstances. Unless there exists an evidence of medical or emergency situation, incomplete grades will not be given.

11. Special course requirements

Course Delivery Method: This course is delivered online and live through Cisco Webex, at the hours and days mentioned above. The students are expected to join the live class and participate at every scheduled class session. All course material and exams would be delivered through Canvas. The student must log into Canvas with their FAU ID and Password to access the materials/assignments in this course.

Exam Administration Method: All quizzes will be held using LockDown Browser and/or Respondus Monitor, or similar features, as determined by the instructor. The midterm and final exams would administered by HonorLocks. The details would be laid out by the instructor prior to the examination. The students must ensure to install the necessary software add-ons to their computers prior to the examination dates.

Technology Requirements: The students are required to have their own personal computers which must be equipped with speakers, microphones, and webcams. The students must have access to reliable broadband internet connection throughout the semester.

Course Assessments/Assignments and Grading Policy: All assignments, homework, projects, programs, quizzes, and exams in this course must be individual effort. All programming assignments are individual work, the best way to learn how to program is to write your own code. Sharing code is considered cheating. Sharing code includes posting completed work before the assignment official deadline onto sites, emailing code to other students, allowing any access to your work before the official deadline has passed. Other code sharing offenses include submitting another person's work as your own, this includes taking code off sites in the internet. Modifying code and submitting it as your own is a fraudulent practice—specifically, plagiarism— and is no different than copying paragraphs of information from a book or journal article and calling it your own. Make sure that you work independently and submit only your own code. We do have access to software that can easily detect plagiarism, and students would be given zero automatically.

Other Matters: Periodic quizzes would be administered throughout the semester to ensure that the students are on track with the material. The quizzes would be taken on Canvas. Once the grades are published for any assignment, lab, exam or quiz, the students are given one week time to report to the instructor any concerns or questions regarding that grade. Discussion boards are a great way to communicate with the entire class, and answer course-related questions. All questions must be posted publicly through Canvas discussion boards, so other students also benefit from the answers. Only personal or confidential matters should be sent via email to the professor, all others will be ignored.

12. Classroom etiquette policy

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

Plagiarism is unacceptable in the University community. Academic work must be an original work of your own thought, research, or self-expression. When students borrow ideas, wording, or organization from another source, they must 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.

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.

Disruptive behavior is defined in the FAU Student Code of Conduct as "... activities which interfere with the educational mission within classroom." Students who disrupt the educational experiences of other students and/or the instructor's course objectives in a face-to-face or online course 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.

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. Attendance policy statement

Since the course is online, you should access the course at regularly to ensure you do not miss pertinent postings, messages, or announcements. It is imperative that you meet course deadlines and stay active in discussion boards. If you are experiencing major illness, absences due to University duties, or other large-scale issues, contact the instructor immediately to formulate a resolution.

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.

14. 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

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

<p>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/.</p>
<p>15. Counseling and Psychological Services (CAPS) Center</p>
<p>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/</p>
<p>16. Code of Academic Integrity policy statement</p>
<p>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. If your college has particular policies relating to cheating and plagiarism, state so here or provide a link to the full policy—but be sure the college policy does not conflict with the University Regulation.</p>
<p>17. Required texts/reading</p>
<p>To reduce costs for our students, we strongly encourage you to explore the adoption of open educational resources (OER), textbooks and other materials that are freely accessible. We also encourage you to clearly state in the syllabus if course materials are available on reserve in the Library.</p>
<p>N/A</p>
<p>18. Supplementary/recommended readings</p>
<p>Cryptography Theory and Practice (4th edition), Stinson, Chapman & Hall/CRC. Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC. Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC.</p>

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

19. 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

From:Rainer Steinwandt <RSTEINWA@fau.edu>
Sent:Thursday, November 5, 2020 10:54 AM
To:Mihaela Cardei <mcardei@fau.edu>
Cc:Hanqi Zhuang <zhuang@fau.edu>
Subject:RE: CEECS - Course Perquisite Changes

Hello,

Sounds good. The proposed prerequisite of "Graduate Standing" makes the courses accessible to our graduate students, which is very welcome. There are no concerns from math w.r.t. this change. Thanks for checking.

Best,
Rainer

From:Mihaela Cardei <mcardei@fau.edu>
Sent:Thursday, November 5, 2020 10:50 AM
To:Rainer Steinwandt <RSTEINWA@fau.edu>
Cc:Hanqi Zhuang <zhuang@fau.edu>
Subject:CEECS - Course Perquisite Changes

Hello Dr. Steinwandt,

CEECS department is changing prerequisites of the following graduate courses which are listed in the Cyber Security Certificate.

CDA5326 Cryptographic Engineering
CIS5371 Practical Aspects of Modern Cryptography

The prerequisites are changed to Graduate Standing.

Changing of the prerequisites for these courses were discussed in UGPC yesterday November 4th, and the UGPC committee asked us to check with the other colleges where we have joint interdisciplinary programs. The next meeting, UGC, is on November 13 from 10:00 AM.

Please let us know if Mathematical Sciences has any objections to these prerequisite changes.

Best regards,
Mihaela Cardei

From:Kevin Wagner <kwagne15@fau.edu>
Sent:Thursday, November 5, 2020 10:26 AM
To:Mihaela Cardei <mcardei@fau.edu>
Cc:Hanqi Zhuang <zhuang@fau.edu>; Taghi Khoshgoftaar <khoshgof@fau.edu>
Subject:Re: MS DSA Steering Committee

Fine with me.

KW

Kevin M. Wagner, J.D., PhD
Professor and Chair, Department of Political Science
President, FAU Faculty Senate
Trustee, FAU Board of Trustees
Director of the Jack Miller Forum
Dorothy F. Schmidt College of Arts and Letters
Florida Atlantic University
777 Glades Road
Boca Raton, FL 33431
tel: 561-252-1794
fax: 561-297-2997
kwagne15@fau.edu
Twitter: @kevinwagnerphd
www.fau.edu/politicalscience



Florida has a very broad public records law. As a result, any written communication created or received by Florida Atlantic University employees is subject to disclosure to the public and the media, upon request, unless otherwise exempt. Under Florida law, e-mail addresses are public records.

On Thu, Nov 5, 2020 at 10:21 AM Mihaela Cardei <mcardei@fau.edu> wrote:
Hello Dr. Wagner,

CEECS department is changing the prerequisites for the following courses which are listed in the MS DSA program:

CORE course in MS DSA:
CAP6673: Data Mining and Machine Learning

ELECTIVE courses in MS DSA:
CAP5615: Introduction to Neural Networks
CAP6315: Social Networks and Big Data Analytics

CAP6619: Deep Learning
CAP6776: Information Retrieval
CAP6777: Web Mining
CEN6405: Computer Performance Modeling

The prerequisites are changed as follows:
6000 level courses - change to no prerequisites
5000 level courses - change to Graduate Standing

These courses were discussed in UGPC yesterday November 4th, and the UGPC committee asked us to check with MS DSA Steering Committee if they have any objections. The next meeting, UGC, is on November 13 from 10:00 AM.

Please let us know if the MS DSA Steering Committee has any objections.

Best regards,
Mihaela Cardei

From:Tamara Dinev <tdinev@fau.edu>
Sent:Thursday, November 5, 2020 10:41 AM
To:Mihaela Cardei <mcardei@fau.edu>
Cc:Hanqi Zhuang <zhuang@fau.edu>
Subject:RE: CEECS - Course Perquisite Changes

Thank you Dr. Cardei. I will come back soon

Best Regards:
Tamara

=====
Tamara Dinev, Ph.D., Department Chair and Professor
Dean's Distinguished Research Fellow
Department of Information Technology and Operations Management, FL 219
College of Business, Florida Atlantic University
Boca Raton, Florida 33431
tel. (561) 297-3181, email: tdinev@fau.edu
Google Scholar:<https://scholar.google.com/citations?user=YH8QZ-YAAAAJ&hl=en>

From:Mihaela Cardei <mcardei@fau.edu>
Sent:Thursday, November 5, 2020 10:35 AM
To:Tamara Dinev <tdinev@fau.edu>
Cc:Hanqi Zhuang <zhuang@fau.edu>
Subject:CEECS - Course Perquisite Changes

Hello Dr. Dinev,

CEECS department is changing prerequisites of the following graduate courses which are listed in the MS ITM and/or Big Data Analytics Certificate.

MS ITM:

CEN 5035 is a core in CEECS concentrations only.

Electives: CAP 5615, CAP 6315, CAP 6619, CAP 6640, CAP 6673, CAP 6776, CAP 6777, CEN 6405, CEN 5086

Big Data Certificate:

CAP 5615, CAP 6315, CAP 6619, CAP 6640, CAP 6673, CAP 6776, CAP 6777, CEN 6405.

The prerequisites are changed as follows:

6000 level courses - change to no prerequisites

5000 level courses - change to Graduate Standing

These courses were discussed in UGPC yesterday November 4th, and the UGPC committee asked us to check with the other colleges where we have joint interdisciplinary programs. The next meeting, UGC, is on November 13 from 10:00 AM.

Please let us know if ITOM has any objections to these prerequisite changes.

Best regards,
Mihaela Cardei