FLORIDA ATLANTIC UNIVERSITY

COURSE CHANGE REQUEST
Undergraduate Programs

Department Electrical Engineering and Computer Science

College Engineering and Computer Science

UUPC Approval 4/21/2025
UFS Approval _____
SCNS Submittal _____
Confirmed _____
Banner Posted _____
Catalog _____

***Current* Course Prefix and Number**	CDA4321	***Current* Course Title**	Intro to Cryptographic Engineering

*Syllabus must be attached for **ANY** changes to current course details. See Template. 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:**

Change WAC/Gordon Rule status**

Add ☐ **Remove** ☐

Change General Education Requirements***

Add ☐ **Remove** ☐

*See Definition of a Credit Hour.

**WAC/Gordon Rule criteria must be indicated in syllabus and approval attached to this form. See WAC Guidelines.

***GE criteria must be indicated in syllabus and approval attached to this form. See Intellectual Foundations Guidelines.

Change description to:

Change prerequisites/minimum grades to:
COP 3275C (Minimum grade of C or better)

Change corequisites to:

Change registration controls to:

Please list existing and new pre/corequisites, specify AND or OR and include minimum passing grade (default is D-).

Effective Term/Year for Changes:	Spring 2026	**Terminate course? Effective Term/Year for Termination:**	

Faculty Contact/Email/Phone

Approved by		***Date***
Department Chair	Hai Kalva	3/12/2025
College Curriculum Chair	Galan Liu	4/10/25
College Dean		4.11.25
UUPC Chair	Korey Sorge	4/21/2025
Undergraduate Studies Dean	Dan Messoff	4/21/2025
UFS President		
Provost		

Email this form and syllabus to mjenning@fau.edu seven business days before the UUPC meeting.

FLORIDA ATLANTIC UNIVERSITY

CDA 4321-001 14100

Intro to Cryptographic Engineering

Date: Wednesday 4:00 PM - 5:50 PM
Building: Engineering East Boca **Room:** 207

Date: Wednesday 6:00 PM - 8:00 PM
Building: Engineering East Boca **Room:** 207

3 Credit(s)

Fall 2025 - 1 Full Term

Instructor Information

Reza Azarderakhsh
Email: razarderakhsh@fau.edu
Office: EE313
Office Hours: W 3-4pm
Phone:

TA Name: Zee Fisher and Aimee Lauclastra
Office:
Office Hours:
Telephone:
Email:

Course Description

Introduction to Cryptographic Engineering
Prerequisite: COP 3275C (Minimum grade of C or better)
This course is devoted to the state-of-the-art in cryptographic hardware/software and embedded systems. Students learn about computational algorithms and architecture of the cryptographic devices. Students also re-learn programming of cryptographic primitives on ASM and C on PC or embedded devices.

This course provides application perspective of cryptography and focuses on the computations, engineering, and secure implementations. This is a course for students interested in hardware and software design in industry and real-world security and cryptographic applications. The course is devoted to the state-of-the-art in cryptographic software and embedded systems. The students will learn about computational algorithms and architectures as well as about cryptanalysis of the cryptographic devices. The students will re/learn programming of cryptographic primitives on C, and hardware. Real world applications include implementations on IoT devices.

Prerequisites/Corequisites

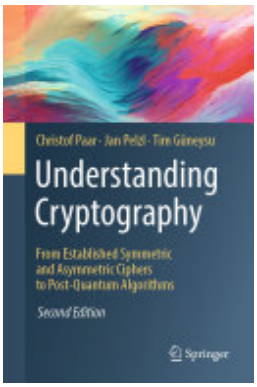
Prerequisite(s): The following course:

- COP 3275C (Minimum grade of C or better)

Instructional Method

In-Person
Traditional concept of in person. Mandatory attendance is at the discretion of the instructor.

Required Texts/Materials



Understanding Cryptography
ISBN: 9783662690079
Authors: CHRISTOF. PELZL PAAR (JAN. GUNEYSU, TIM.), Jan Pelzl, Tim Güneysu
Publisher: Springer Nature
Publication Date: 2024-01-01

Course Objectives/Student Learning Outcomes

This is a cryptography engineering course. The students learn about embedding cryptographic algorithms and architectures into security products such as embedded devices where they can use programming to prototype to verify and demonstrate concepts. They will learn about implementations on hardware and software platforms including CPUs and MCUs.

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 that do not impede their exercise. To ensure these rights, faculty members have the prerogative to:

• Establish and implement academic standards.

• Establish and enforce reasonable behavior standards in each class.

• Recommend disciplinary action for students whose behavior may be judged as disruptive under the Student Code of Conduct University Regulation 4.007.

Disability Policy

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/.

Course Evaluation Method

5 Programming Assignments in Labs (13% each): 65%

Final Exam: 35%

Code of Academic Integrity

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.

NA

Attendance Policy Statement

Students are expected to attend all 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.

Religious Accommodation Policy Statement

In accordance with the 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 regarding admissions, registration, class attendance, and the scheduling of examinations and work assignments. University Regulation 2.007, Religious Observances, sets forth this policy for FAU and may be accessed on the FAU website at www.fau.edu/regulations.

Any student who feels aggrieved regarding religious accommodations may present a grievance to the executive director of The Office of Civil Rights and Title IX. Any such grievances will follow Florida Atlantic University's established grievance procedure regarding alleged discrimination.

Time Commitment Per Credit Hour

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 are required for Summer Semesters, which usually have a shortened timeframe. Fully Online courses, hybrid, shortened, intensive format courses, and other non-traditional modes of delivery will demonstrate equivalent time and effort.

Course Grading Scale

Letter Grade	Percentage
A	100 - 94%
A-	< 94 - 90%

Letter Grade	Percentage
B+	< 90 - 87%
B	< 87 - 83%
B-	< 83 - 80%
C+	< 80 - 77%
C	< 77 - 73%
C-	< 73 - 70%
D+	< 70 - 67%
D	< 67 - 63%
D-	< 63 - 60%
F	< 60 - 0%

Grade Appeal Process

You may request a review of the final course grade when you believe that one of the following conditions apply:

• There was a computational or recording error in the grading.

• The grading process used non-academic criteria.

• There was a gross violation of the instructor's own grading system.

University Regulation 4.002 of the University Regulations contains information on the grade appeals process

Policy on Make-up Tests, Late work, and Incompletes

Penalties for late assignment submission will be 5% per day. 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.

Penalties for late project submission will be 25% per day. The student will get zero after 4 days.

Policy on the Recording of Lectures

Students enrolled in this course may record video or audio of class lectures for their own personal educational use. A class lecture is defined as a formal or methodical oral presentation as part of a university course intended to present information or teach students about a particular subject. Recording class activities other than class lectures, including but not limited to student presentations (whether individually or as part of a group), class discussion (except when incidental to and incorporated within a class lecture), labs, clinical presentations such as patient history, academic exercises involving student participation, test or examination administrations, field trips, and private conversations between students in the class or between a student and the lecturer, is prohibited. Recordings may not be used as a substitute for class participation or class attendance and may not be published or shared without the written consent of the faculty member. Failure to adhere to these requirements may constitute a violation of the University's Student Code of Conduct and/or the Code of Academic Integrity.

Artificial Intelligence Preamble

FAU recognizes the value of generative AI in facilitating learning. However, output generated by artificial intelligence (AI), such as written words, computations, code, artwork, images, music, etc., for example, is drawn from previously published materials and is not your own original work.

FAU students are not permitted to use AI for any course work unless explicitly allowed to do so by the instructor of the class for a specific assignment. **[Policy 12.16 Artificial Intelligence]**

Class policies related to AI use are decided by the individual faculty. Some faculty may permit the use of AI in some assignments but not others, and some faculty may prohibit the use of AI in their course entirely. In the case that an instructor permits the use of AI for some assignments, the assignment instructions will indicate when and how the use of AI is permitted in that specific assignment. It is the student's responsibility to comply with the instructor's expectations for each assignment in each course. When AI is authorized, the student is also responsible and accountable for the content of the work. AI may generate inaccurate, false, or exaggerated information. Users should approach any generated content with skepticism and review any information generated by AI before using generated content as-is.

If you are unclear about whether or not the use of AI is permitted, ask your instructor before starting the assignment.

Failure to comply with the requirements related to the use of AI may constitute a violation of the **Florida Atlantic Code of Academic Integrity, Regulation 4.001.**

Proper Citation: If the use of AI is permitted for a specific assignment, then use of the AI tool must be properly documented and cited. For more information on how to properly cite the use of AI tools, visit

https://fau.edu/ai/citation

AI Language Specific To This Course

- AI Encouraged: The use of AI to assist in work assigned in this specific course is encouraged for various purposes. The instructor hereby permits the use of AI to assist in work assigned for this course, unless the instructor expressly indicates AI is not permitted on a particular assignment. Use must be properly documented and cited per instructor guidelines (https://fau.edu/ai/citation).

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 therapy, group therapy, and crisis services, to name a few - offered to help improve and maintain emotional well-being. For more information, go to http://www.fau.edu/counseling/

Student Support Services and Online Resources

- Center for Learning and Student Success (CLASS)
- Counseling and Psychological Services (CAPS)
- FAU Libraries
- Math Learning Center
- Office of Information Technology Helpdesk
- Center for Global Engagement
- Office of Undergraduate Research and Inquiry (OURI)
- Science Learning Center
- Speaking Center
- Student Accessibility Services
- Student Athlete Success Center (SASC)
- Testing and Certification
- Test Preparation
- University Academic Advising Services
- University Center for Excellence in Writing (UCEW)

- Writing Across the Curriculum (WAC)

Course Topical Outline

Weekly Schedule	Topics
Week 01	Introduction to Computer Security and Cryptography
Week 02	Mathematical background: Number theory, abstract algebra, Finite fields.
Week 03	Finite Field, prime Field, modular arithmetic, quadratic fields and arithmetic. Lab Assignment #1
Week 04	Finite Field, binary fields, binary extension fields, representation of field elements, polynomial basis, normal basis and Gaussian normal basis.
Week 05	Multiplication over finite fields: super-serial, bit-level, digit-level, bit-parallel architectures
Week 06	Multiplication over finite field: Karatsuba, subquadratic multipliers, systolic array multipliers, hybrid-double multipliers. Assignment #2
Week 07	Multiplicative inversion, Fermatt's little theorem, extended Euclidean Algorithm over prime and binary fields.
Week 08	Exponentiation over finite field, trace and half trace function over finite fields, constant-time and non-constant- time implementations.
Week 09	Public key cryptography, Diffie-Hellman key exchange, RSA, Elliptic curve cryptography (ECC). Assignment #3
Week 10	Implementations of RSA and Diffie-Hellman over binary fields and prime fields. Introduction to AES and Hash Functions.
Week 11	Elliptic curves, generic curves, Montgomery curves, Edwards curves, Hassian and Huff curves.
Week 12	Implementations of Elliptic Curve Cryptography over prime fields, Group law, group operations, point multiplication, coordinates systems. Assignment #4
Week 13	Implementations of Elliptic Curve Cryptography over binary fields (polynomial basis and normal basis). Side-channel attacks analysis, secure implementations, and countermeasures.
Week 14	Digital Signature algorithms (ECDSA, El Gamal) and implementations, Security-level and key size, performance analysis on hardware and software platforms
Week 15	Introduction to quantum computation and post-quantum cryptography: Lattice

	based cryptography and code-based cryptography. Assignment #5

Title IX Statement

In any case involving allegations of sexual misconduct, you are encouraged to report the matter to the University Title IX Coordinator in the Office of Civil Rights and Title IX (OCR9). If University faculty become aware of an allegation of sexual misconduct, they are expected to report it to OCR9. If a report is made, someone from OCR9 and/or Campus Victim Services will contact you to make you aware of available resources including support services, supportive measures, and the University's grievance procedures. More information, including contact information for OCR9, is available at **https://www.fau.edu/ocr9/title-ix/**. You may also contact Victim Services at **victimservices@fau.edu** or 561-297-0500 (ask to speak to an Advocate) or schedule an appointment with a counselor at Counseling and Psychological Services (CAPS) by calling 561-297-CAPS.