FAU

FLORIDA
ATLANTIC
UNIVERSITY

COURSE CHANGE REQUEST
Graduate Programs

UGPC Approval ______________
UFS Approval ______________
SCNS Submittal ______________
Confirmed ______________
Banner ______________
Catalog ______________

Department CEECS

College Engineering & Computer Science

***Current* Course Prefix and Number** CDA 5326

***Current* Course Title** Cryptographic Engineering

*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 □ **Remove** □

* Review Provost Memorandum
** Academic Service Learning statement must be indicated in syllabus and approval attached to this form.

Change description to:

Change prerequisites/minimum grades to:

Graduate standing for CEECS students, and instructor's approval for students from other major.

Change corequisites to:

Change registration controls to:

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	***Date***
Department Chair Hanqi Zhuang Digitally signed by Hanqi Zhuang Date: 2020.10.21 15:40:01 -04'00'	
College Curriculum Chair Francisco Presuel-Moreno 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 12:43:19 -04'00'	
College Dean MCardei Digitally signed by Mihaela Cardei DN: cn=Mihaela Cardei, o=Florida Atlantic University, ou, email=mcardei@fau.edu, c=US Date: 2020.10.25 19:25:25 -04'00'	10/25/2020
UGPC Chair	
UGC Chair	
Graduate College Dean	
UFS President	
Provost	

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

Cryptographic Engineering, CDA 5326	3 credit hours

2. Course prerequisites, corequisites, and where the course fits in the program of study

Prerequisites: Graduate standing for CEECS students, and instructor's approval for students from other major.

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

This course provides an 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.

7. Course objectives/student learning outcomes/program outcomes

Course objectives	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 FPGAs and CPUs.

8. Course evaluation method

5 Programming Assignments (9% each):	45%
Projects:	25%
Final Exam:	30%

For the project, the students will identify a scientific paper for review and implementations. The students will prepare a 10-page technical report to discuss the problem in the paper, the methodology applied, implementations techniques in the paper, and their results. In addition, the students may propose a new approach to address the problem and compare their results with the methods found in the paper. The students will deliver a 15-minutes presentation and present their final work to the class. The project will be implemented in four phases: (i) proposing/identifying a paper, (ii) review of the paper, (iii) implementations in a target platform, (iv) final report and presentations. The assignments in this class will be programming with the help of the TA/Instructor in the class or lab.

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

Penalties for late assignment submission will be 10% 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.

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.

FAU course management system (Canvas) will be the official communication tool between the instructor and the students, and it is the student’s responsibility to regularly check the course shell for updates and announcements. This includes unforeseen changes to assignment/project deadlines. It is the student’s responsibility to inform the professor, within the first week of class, of any conflict with important course dates. No accommodation will be made if these conflicts are not brought to our attention within the first week.

Students are strongly encouraged to ask questions during class. You may not use a PDA, PPC, laptop, netbook or other computer, IPOD or similar device in-class or during quizzes or exams. Cellular/PCS telephones, pagers, PDAs, etc. must be turned-off or put in vibrate mode during class. If your device disrupts the lecture, you may be asked to leave immediately. Upon a second offense, you will need to explain your actions to the CEECS Department Chair before being allowed to return. If you require an exception to this policy, please see me before creating a disturbance.

Although you are EXPECTED and ENCOURAGED to utilize a study-group, individual and original efforts are expected for all assignments and projects except when otherwise stated.

13. 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.

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 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/

15. 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/

16. 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.

17. Required texts/reading

The course will not follow a particular textbook.

18. Supplementary/recommended readings

Materials will be provided in an ongoing basis. The following references will be optional to follow:

- Cetin Kaya Koc (Editor): Cryptographic Engineering. 1st edition, Springer, 2009
- Paar, Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. 1st edition, Springer, 2009 Hankerson, Menezes and Vanstone, Guide to Elliptic Curve Cryptography (Ch. 2, 3, 5)
- Menezes, van Oorschot and Vanstone, Handbook of Applied Cryptography (Chapters 2 and 14) (Available free online)
- Articles from IEEE Transactions on Computers, CHES/ECC workshops proceedings

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

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. **Assignment #1**
Week 04	Finite Field, binary fields, binary extension fields, representation of field elements, polynomial basis, normal basis and Gaussian normal basis. **Project phase (i)**
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. **Project phase (ii)**
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.

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. **Project Phase (iii)**
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, isogeny-based cryptography, and other candidates. **Assignment #5** Students' project presentations **Project Phase (iv)**