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

1. Course title/number, number of credit hours	
Intro to Cryptographic Engineering, CDA 4321	3 Credits
2. Course prerequisites, corequisites, and where the course fits in the program of study	
COP 2220	
3. Course logistics	
Term: Fall 2020 *Class location and time:* TBA	
4. Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	TBA
5. TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	TBA
6. Course description	
The course is devoted to the state-of-the-art in cryptographic hardware/software and embedded systems. The students will learn about computational algorithms and architectures of the cryptographic devices. The students will re/learn programming of cryptographic primitives on ASM and C on PC or embedded device.	
7. Course objectives/student learning outcomes/program outcomes	
Course objectives	This is an Introduction to 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. The student will be able to measure performance of cryptographic algorithms.
Student learning outcomes & relationship to ABET 1-7 outcomes	
8. Course evaluation method	
5 Programming Assignments (10% each): 50% Homework: 15% Final Exam: 35%	
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. 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.

17. Required texts/reading

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.

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

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

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.
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. Exponentiation over finite field, trace and half trace function over finite fields, constant-time and non-constant- time implementations.
Week 08	Advanced Encryption Standards, Galois Counter Mode, Hash Functions, and Block Cipers **Assignment #3**
Week 09	Public key cryptography, Diffie-Hellman key exchange, RSA, Elliptic curve cryptography (ECC).
Week 10	Implementations of RSA and Diffie-Hellman over binary fields and prime fields. **Assignment #4**
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.
Week 13	Implementations of Elliptic Curve Cryptography over binary fields (polynomial basis and normal basis). Side-channel attacks analysis, secure implementations, and countermeasures. **Assignment #5**
Week 14	Digital Signature algorithms (ECDSA, El Gamal) and implementations, Security-level and key size, performance analysis on hardware and software platforms
Week 15	Advanced topics for post-quantum cryptography