FLORIDA ATLANTIC UNIVERSITY

# NEW COURSE PROPOSAL
## Graduate Programs

**Department of Computer & Elec. Eng. and Computer Sci**

**College of Engineering and Computer Science**
*(To obtain a course number, contact **erudolph@fau.edu**)*

UGPC Approval _____
UFS Approval _____
SCNS Submittal _____
Confirmed _____
Banner Posted _____
Catalog _____

| | | |
|---|---|---|
| **Prefix** CDA **Number** 5637 | *(L = Lab Course; C = Combined Lecture/Lab; add if appropriate)* **Lab Code** | **Course Title** Cryptographic Engineering |
| **Credits** *(Review Provost Memorandum)* 3 | **Grading** *(Select One Option)* **Regular** X **Sat/UnSat** | **Course Description** *(Syllabus must be attached; see Guidelines)* 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. |
| **Effective Date** *(TERM & YEAR)* **FALL 2018** | | |

| **Prerequisites** | **Corequisites** | **Registration Controls** *(Major, College, Level)* |
|---|---|---|
| Discrete Mathematics (MAD 2104) | N/A | Graduates, seniors (Eng. & Com. Sci, or College of Science) |

***Prerequisites, Corequisites and Registration Controls are enforced for all sections of course***

| | |
|---|---|
| **Minimum qualifications needed to teach course:** Member of the FAU graduate faculty and has a terminal degree in the subject area (or a closely related field.) | **List textbook information in syllabus or here** No Textbook required. |
| **Faculty Contact/Email/Phone** Reza Azarderakhsh/razarderakhsh@fau.edu/(561) 297-4980 | **List/Attach comments from departments affected by new course** Charles E. Schmidt College of Science, Department of Mathematical Sciences |

| ***Approved by*** | ***Date*** |
|---|---|
| Department Chair Nurgun Erdol | 11/14/2017 |
| College Curriculum Chair M Candeli | 11/16/2017 |
| College Dean | 11/20/2017 |
| UGPC Chair | |
| Graduate College Dean | |
| UFS President | |
| Provost | |

Email this form and syllabus to UGPC@fau.edu one week before the UGPC meeting.

*FAUnewcourseGrad, created August 2016*

GRADUATE COLLEGE
NOV 28 2017
Received

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

| **1. Course title/number, number of credit hours** | |
|---|---|
| Cryptographic Engineering, CDA 5637 | 3 credit hours |
| **2. Course prerequisites, corequisites, and where the course fits in the program of study** | |
| Discrete Mathematics (MAD 2104) | |
| **3. Course logistics** | |
| *Term*: Fall 2018<br>*Class location and time* TBD | |
| **4. Instructor contact information** | |
| *Instructor's name*<br>*Office address*<br>*Office Hours*<br>*Contact telephone number*<br>*Email address* | Reza Azarderakhsh<br>EE314<br>TBD<br>(561) 297-4980<br>razarderakhsh@fau.edu |
| **5. TA contact information** | |
| *TA's name*<br>*Office address*<br>*Office Hours*<br>*Contact telephone number*<br>*Email address* | |
| **6. Course description** | |
| 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 hardware/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 ASM, C, and hardware (using VHDL). Real world applications include implementations on cellphones, FPGA, and IoT devices with 8-bit/16-bit microcontrollers. | |
| **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. |
| | |

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

## 8. Course evaluation method

| | |
|---|---|
| 5 Programming Assignments (9% each): 45%<br>Project: 55% | 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 will 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. 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)—in Boca Raton, SU 133 (561-297-3880); in Davie, LA 131 (954-236-1222); or in Jupiter, SR 111F (561-799-8585) —and follow all SAS procedures.

## 14. Honor code policy

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 unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and place high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. See University Regulation 4.001 at
www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf

## 15. Required texts/reading

The course will not follow a particular textbook.

## 16. 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

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

**17. 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)** |

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

On Sat, Oct 28, 2017 at 12:56 PM, Reza Azarderakhsh <razarderakhsh@fau.edu> wrote:

Dear. Dr. Steinwandt,

The Department of Computer & Electrical Engineering and Computer Science (CEECS) is proposing a new course: Cryptographic Engineering. Please see the attached syllabus for this course. We need your approval that Department of mathematics has no objection to this new course proposal for CEECS and inclusion in Cyber Security Graduate Certificate. Could you please review the syllabus and email me your decision on approval at your earliest convenience?

Thanks and regards,

Reza

--

Reza Azarderakhsh, Ph.D.
Associate Editor, IEEE Transactions on Circuits and Systems I (TCAS-I)
Assistant Professor and I-SENSE Fellow
Department of Electrical & Computer Engineering and Computer Science
Florida Atlantic University
777 Glades Road, Room EE 314
Boca Raton, FL 33431-0991
Phone: +1 (561) 297-4889
Email: razarderakhsh@fau.edu
Web: http://faculty.eng.fau.edu/azarderakhsh/

On Sun, Oct 29, 2017 at 5:16 PM, Rainer Steinwandt <RSTEINWA@fau.edu> wrote:

Hi, Reza,

Looks like an interesting course-- our department has no objections. Thanks for checking.

Best wishes,
Rainer