Introduction to Security and Cryptography
Course Syllabus

1. Course title/number, number of credit hours	
Introduction to Security and Cryptography EGN 1935	3 credit hours
2. Course prerequisites, corequisites, and where the course fits in the program of study	
Programming in Java or C/C++ is required. Knowledge of algebra and calculus would be helpful. The instructor will review necessary math materials.	
3. Course logistics	
Term: Summer 2016 *Class location and time*: The course will be held for 3 weeks (Jun 13~July 01) on MWF (9:30 am to 4:30 pm), during summer 2016. Blackboard will be used for posting assignments, material, and grades.	
4. Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	Mehrdad Nojoumian EE96, Room 530 Tuesdays and Thursdays: 01:00 to 03:00. 561.297.3411 mnojoumian@fau.edu
5. TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	TBD
6. Course description	
This course enables the students to (a) become familiar with hot topics in cybersecurity as well as ongoing challenges, (b) learn fundamental concepts of computer security, (c) discover modern cryptographic tools, and finally, (d) utilize these techniques in computing systems. Furthermore, after passing this course, the students will be able to identify, formulate, and solve inspiring cybersecurity problems. One of the major components of this course is the team project. This will also establish a fascinating platform for the students to collaborate, discover and solve challenging problems.	
7. Course objectives/student learning outcomes/program outcomes	
Course objectives	Enable the students to learn fundamental concepts of computer security and cryptography and utilize these techniques in computing systems.
Student learning outcomes & relationship to ABET a-k objectives	**Outcome 2:** A working knowledge of fundamentals. Graduates will have knowledge of mathematics and science fundamentals. They will be able to combine these basics with their knowledge of computer programming to identify, formulate, and solve security and crypto problems. **Outcome 5:** An ability to function on multi-disciplinary teams. Graduates will be able to function effectively on teams using their knowledge of team dynamics, team communication and social norms.

	Outcome 6: An ability to communicate effectively. Graduates will be able to communicate their ideas and results to diverse audiences using their knowledge of written, oral, and graphical communication. **Objectives 1:** Function effectively in their discipline of practice, and will continue their education through graduate/professional studies and/or participation in professional seminars and societies. **Objectives 2:** Utilize their training and experience in creative and design processes toward their job functions.

8. Course evaluation method

Subject to changes: Homework: 10% Exam: 30% Presentation: 10% Demo of the Project Team Project: 50% Team of 2~3 Students Class Participation: 5% Bonus	**Team Project:** Students will be involved in a team project, i.e., implementation of security protocols and cryptographic schemes. This project will provide an excellent opportunity for the students to explore computer science, and more specifically cybersecurity, as the most promising career choice.

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."
Note: The minimum grade required to pass the course is D.

10. Policy on makeup tests, late work, and incompletes

All assignments are due at 10:00 am 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. 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.

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.

13. Disability policy statement

In compliance with the Americans with Disabilities Act, students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca Raton campus, SU 133 (561) 297-3880 and follow all OSD procedures.

Introduction to Security and Cryptography
Course Syllabus

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 http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf

15. Required texts/reading

The instructor will provide all the necessary materials and lecture notes.

16. Supplementary/recommended readings

Computer Security: Principles and Practice (3rd edition), Stallings and Brown, Pearson.
Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC.

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

The following topics will be covered in 9 lectures during 3 weeks (subject to minor changes):

- Preliminary Materials and Mathematical Foundations of Cryptography:

  Jun 13: Terminologies, Security Models and Definitions, Complexity, and Modular Arithmetic.
  Jun 15: Prime Numbers, GCD, LCM, (Extended) Euclidian Algorithm, and Multiplicative Inverse.
  Jun 17: Congruence, Primitive Roots, Discrete Log, Random Number Generators, and Functions.

- Modern Cryptography:

  Jun 20: Symmetric/Private-Key Encryption: DES and AES Block Ciphers.
  Jun 22: Asymmetric/Public-Key Encryption: RSA, ElGamal and Rabin Schemes.
  Jun 24: Security Protocols: Secret Sharing, Hash Functions and Digital Signatures.

- Hot Topics in Cybersecurity:

  Jun 27: Exam: Security & Crypto Materials, Digital Currencies (Bitcoin), and Sealed-Bid Auctions.
  Jun 29: Modern Attacks (Cold-Boot Attack), and Hijacking/Hacking Cars and Drones.
  July 01: Team Project Demo and Presentation - Each Team Consists of 2~3 Students.