Introduction to Security and Cryptography
Course Syllabus

1. Course title/number, number of credit hours	
Introduction to Security and Cryptography COT 4930	3 credit hours
2. Course prerequisites, corequisites, and where the course fits in the program of study	
Prerequisites: MAD2104 and COP3014. Knowledge of linear algebra, number theory and computer programming would be of great help. The instructor also reviews some of the necessary background materials.	
3. Course logistics	
Term: Spring 2016 *Class location and time*: Online Lectures and FL 404, Tuesdays and Thursdays: 03:30 ~ 04:50.	
4. Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	Mehrdad Nojoumian EE96, Room 530 Tuesdays and Thursdays: 10:00 ~ 12:00. 561.297.3411 mnojoumian@fau.edu
5. TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	N/A
6. Course description	
This is a course on computer security and cryptographic algorithms. The following components are covered in the course: (a) Overview of computer security concepts (b) Computer security technology and principles, (c) Software security and trusted systems, (d) Management issues, (e) Cryptographic algorithms, and (f) Network security.	
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 math and science fundamentals. They will be able to combine these basics with their knowledge of experimental methodologies to identify, formulate, and solve engineering problems. **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 & Participation: Presentation: Final Project: Midterm & Final Exams:	 Bonus up to 10% 20% 30% 50%	**Project:** students are supposed to select one of the following options: (a) develop new models and protocols, (b) improve existing cybersecurity systems, (c) implement existing security systems, or (d) prepare a survey on a hot cybersecurity topic.

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 11:00 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.

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

Computer Security: Principles and Practice (3rd edition), Stallings and Brown, Pearson.

16. Supplementary/recommended readings

Security in Computing (5th edition), Pfleeger, Pfleeger and Margulies, Pearson.
Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC.
Cryptography Theory and Practice (3rd edition), Stinson, Chapman & Hall/CRC.
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 concepts and topics will be covered with different levels of emphasis. Some topics will be covered in-depth and some other topics will be reviewed briefly.

1. Overview of Computer Security Concepts
2. Computer Security Technology and Principles
   - Cryptographic Tools
   - User Authentication
   - Access Control
   - Database and Cloud Security
   - Malicious Software (Trojans, Phishing, Spyware)
   - Denial-of-Service Attacks
   - Intrusion Detection
   - Firewalls and Intrusion Prevention Systems
3. Software Security and Trusted Systems
   - Buffer Overflow
   - Software Security
   - Operating System Security
   - Trusted Computing and Multilevel Security
4. Management Issues
   - IT Security Management and Risk Assessment
   - IT Security Controls, Plans and Procedures
   - Physical and Infrastructure Security
   - Human Resources Security
   - Security Auditing
   - Legal and Ethical Aspects
5. Cryptographic Algorithms
   - Symmetric Encryption and Message Confidentiality
   - Public-Key Cryptography and Message Authentication
6. Network Security
   - Internet Security Protocols and Standards
   - Internet Authentication Applications
   - Wireless Network Security