Spring 2023

CS 408 – Cryptography and Internet Security

Section: 001

Instructor: Fuad Hamidli

Email: fuad.hamidli@njit.edu

Course website (on CANVAS): https://njit.instructure.com/courses/30810

Office hours: Monday 5:30-6:30 pm (Newark GITC 4202)

Also, by appointment via email.

Prerequisites:

Prerequisites: CS 351 (at least grade C)

Textbook:

"Introduction to Cryptography with Coding Theory (third ediiton)", by Wade Trappe and Lawrence Washington (Optional)

Description:

This is an introductory course on cryptography and Internet security.

The course covers basic security and cryptographic concepts, together with principles of secure communication over the Internet.

This course also builds the foundations for other (more advanced) security courses. A tentative list of topics to be covered follows:

- classical cryptosystems, the one-time pad
- block ciphers (DES, AES)
- stream ciphers
- basic number theory notions
- public-key cryptography (RSA, Diffie-Hellman, ElGamal)
- definitions of security
- random number generation
- cryptographic hash functions

- message authentication codes
- digital signatures (RSA, ElGamal, DSA, Schnorr)
- public key infrastructure, PGP
- authentication protocols, key establishment protocols
- Kerberos
- SSL, IPsec
- zero-knowledge protocols
- secure multi-party computation
- identity-based encryption
- threshold cryptography
- Web and Internet security

Grading Policy:

2 (written) Assignments	20%
2 (in class) Quizzes:	24%
Midterm exam:	26%
Final exam:	30%
1 Presentation Project (optional)	10%

Extra credit will be given for active participation in discussions during the class (up to 10%). The quizzes and exams are closed book unless specified otherwise.

Learning Outcomes:

After completing the course, students will be able to:

- Understand the role of cryptography in securing computer systems and computer networks. Get familiar with the main types of attacks that may occur in computer systems and networks.
- Understand the various models to evaluate the security of cryptographic, including the notion of provable security. Interpret security guarantees.

- Understand the various security goals for communication over an insecure network. Identify the appropriate types of cryptographic primitives that should be used to achieve each of these goals.
- Gain familiarity with the number theoretic foundations of modern cryptography. Describe cryptographic primitives and identify why such primitives are crucial to building secure systems.
- Assess the level of security provided by a cryptographic protocol.
- Build new cryptographic protocols in order to achieve security guarantees for a diverse set of real-world scenarios.
- Apply theoretical concepts in practice by using a programming language and standard cryptographic libraries to implement a cryptographic protocol.

Honor Code:

Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to protect your educational investment by knowing and following the academic code of integrity policy that is found at:

http://www5.njit.edu/policies/sites/policies/files/academic-integrity-code.pdfLinks to an external site..

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. ***Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university.*** *If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu*

Note in particular that cheating on exams, copying homework assignments and exam papers, and plagiarizing (in full or in part) someone else's work is forbidden.

Collaboration of any kind is PROHIBITED in the exams. As part of projects, students must turn in code or work that has fully been written by him/her and no-one else. Any

submitted text or code (even few lines) obtained through the Internet or otherwise, or is product of someone else's work, risks severe punishment, as outlined by the University; all parties of such interaction receive automatically 0 and grade is lowered by one or two levels. Likewise for Exams, if applicable. The work you submit must be the result of your own mental effort and you must safeguard it from other parties; if you can't protect your home computer, use a Lab (AFS) machine.

Modifications to Syllabus:

The syllabus may be modified at the discretion of the instructor or in the event of extenuating circumstances. Students will be notified in class of any changes to the syllabus.