Cryptography&Computer Security– CSC 73010-01 (56902)

Course Information:

Instructor Information:

- Tzipora Halevi
- thalevi@gc.cuny.edu

Online Course Webpage: ***http://thalevi.github.io/CSC73010***

Hours and location:

Mon 9:30 – 11:30 am	online – zoom link will be sent by email

Course Description:

The course will introduce students to concepts of cryptography and computer security . Students will learn to think like an adversary. They will study how to analyze threats, attacks and vulnerabilities and become familiar with security policies and computer security mechanisms. The course will cover cryptographic concepts and terminology, malware classification and detection, intrusion detection and more. The course will include presentations as well as projects that will give students hands-on experience with information security practices. Upon completing the course, students will have familiarity with key aspects of information risk and security management, as well as skills and roles within the information security industry.

Course Requirements:

Course Textbooks:

Security in Computing fifth edition,
Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, Prentice
Hall imprint, Pearson Education, Inc., 2015.

Recommended book:

Understanding Cryptography: A Textbook for Students and Practitioners, 1st ed.,
Christof Paar, Jan Pelzl, Bart Preneel, 2010 edition

Course Overview:

Introduction to Computer Security and Cryptography: Fundamental Concepts
Primarily a systems perspective

Computer Security layers:

- Operating systems, malicious software, network security, browser security, physical security, security models, applications security
- Risk management
- Interdisciplinary aspects relating to computer security: privacy, ethics, legal issues

Cryptography:

- Asymmetric and symmetric encryption
- Hashing and digital signature
- Passive and active security
- Provable security and cryptographic definitions
- Advanced topics

Course Goals:

- Learning to build secure systems.
- Understanding different potential attacks and their impact
- Gain familiarity with cryptographic concepts and methods

System Security Evaluation: -

Security Goals:

- Threat model:
  - Who is your adversary?
  - What types of attacks might they use?
  - What are their capabilities?
  - What are their limits?
  - What is in and out of scope?
  - Are the security goals achieved?

Computer Security Model:

- Confidentiality, integrity and availability

Course Structure:

Homework:

There will be frequent assignments during the semester covering the topics discussed in class, from the textbook or on-line searches. There will be at least one longer assignment where the student will be expected to write a paper based on their research

Homework solutions must be legible; Difficult-to-read solutions may be marked off or may not be graded entirely. Typing homework is recommended. **No late homework accepted.**

Exams:

There will be a midterm and a final exam. Exams will be given on blackboard.

Class Grading:

Homework: 30%
Exams: 30%
Projects: 40%