CSc 85030 CRN 25405: Cryptography & Computer Security

Prof. Delaram Kahrobaei

Meets Wed., 4:15pm – 6:15pm, Rm. TBA

Course description: http://www.gc.cuny.edu/Page-Elements/Academics-Research-Centers-Initiatives/Doctoral-Programs/Computer-Science/Course-Listings/Fall-2014/Cryptography-Computer-Security.

Description: The Cryptography and Computer Security is an important area that aligns with the mission of the Ph.D. program in Computer Science; i.e., Computer Science professions need to include security by design in the development of cutting edge technologies.

The Center for Strategic and International Studies in Washington estimates the cost to the United States economy due to security breach at about $100 billion a year, let alone the impact of security breach on the national security. It is paramount for our Ph.D. program in Computer Science to train our students to incorporate security and privacy by design into the research and development of cutting edge technologies. This course is an introductory course for the Cryptography and Computer Security new curriculum, and to fill the need of training our students in this area. More importantly, this new course intends to expose our students early on to anticipate and think out of a box, as opposed to being reactionary, in the design of security solutions. In this course, we cover various aspects of modern cryptography and computer security. The topics include number theory, group theory, factoring, public-key encryption and digital signature schemes.

Course Topics:

Introduction

- Cryptography and Modern Cryptography
- The Setting of Private-Key Encryption
- Historical Ciphers and Their Cryptanalysis
- The Basic Principles of Modern Cryptography

Perfectly-Secret Encryption

- Definitions and Basic Properties
- The One-Time Pad
- Limitations of Perfect Secrecy

Number Theory and Cryptographic Hardness Assumptions

- Preliminaries and Basic Group Theory
- Primes, Factoring, and RSA
- Assumptions in Cyclic Groups
- Cryptographic Applications of Number-Theoric Assumptions

Factoring and Computing Hardness Logarithms

- Algorithms for Factoring
- Algorithms for Computing Discrete Logarithms

Public-Key Encryption

- Public-Key Encryption - An Overview
- Definitions
- Hybrid Encryption
- RSA Encryption
- The El Gamal Encryption Scheme
- Security Against Chosen-Ciphertext Attacks
- Trapdoor Permutations

Additional Public-Key Encryption Schemes

- The Goldwasser-Micali Encryption Scheme
- The Rabin Encryption Scheme
- Paillier Encryption Scheme

Digital Signature Schemes

- Digital Signatures - An Overview
- Definitions
- RSA Signatures
- The "Hash-and-sign" Paradigm
- Lamport's One-Time Signature Scheme
- Signature from Collision-Resistant Hashing
- The Digital Signature Standard
- Certificates and Public-Key Infrastructures

Textbook:

Introduction to Modern Cryptography

Authors: Jonathan Katz, Yehuda Lindell

Series: Chapman & Hall/CRC Cryptography and Network Security Series

Publisher: Chapman and Hall/CRC; 1 edition

ISBN-10: 1584885513 ISBN-13: 978-1584885511

Assessment:

- Homework / Project / Attendance & participation 30%
- Midterm 30%
- Final 40%