CIS600: Cryptographic Engineering

MW 10:35-11:55 am, Link 211, Spring 2017

Course description

The course is designed for future cryptography engineers (and scientist). The course theme is to empower students with skills of correctly using cryptographic libraries and building proven secure applications. The course outcome includes:

1. deep understanding of security properties of cryptographic primitives/protocols (e.g. hashes, PKE),
2. knowledge about real-world security protocols and applications (e.g.**blockchain**, **Intel SGX**).
3. hands-on experiences about correct use of cryptographic libraries (e.g.**NaCL**),

The course covers all three aspects in a systematic way (see the course schedule). Note this course is**not** about the mathematical construction of pritimives (e.g. internal working of SHA256).

Instructor

Dr. Yuzhe Tang Office: CST 4-184, [http://ecs.syr.edu/faculty/yuzhe]

Material

Textbook *Introduction to Modern Cryptography* (2nd edition), Jonathan Katz and Yehuda Lindell
Cryptography Engineering: Design Principles and Practical Applications 1st Edition, Niels Ferguson, Bruce Schneier, Tadayoshi Kohno.

Grading

Projects/Exercises (40%), Presentation (30%), Exams (20%)

Course format

Section	Topics	Programming
Cryptographic primitives	Formal security, Secret-key cryptography, Public-key cryptography	EasyCrypt
Security applications	Blockchain, Intel SGX, Kerberos	NACL, OpenSSL