CIS600: Cryptographic Engineering

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, PKC),
2. knowledge about real-world security protocols and applications (e.g.**blockchain**, **Intel SGX**).
3. hands-on experiences about correct use of cryptographic libraries.

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

Class participation (10%), Homework (20%), Labs (35%), Exams (35%)

Late submission policy: 10% off within one day, 40% off within two days, 50% off within three days, 70% off within one week.

Course schedule

Section	**Topics**
Introduction	Formal security
Cryptographic primitives	Secret-key cryptography, Public-key cryptography
Security assumptions	group theory, computational hardness, etc.
Security applications & protocols	Kerberos, PKI & TLS, Blockchain, TEE