CSE539 Applied Cryptography – Syllabus

Catalog Data:
Uses cryptography for secure protocols over networked systems, including signatures, certificates, timestamps, electrons, digital cash, and other multiparty coordination.

Textbook:
None. Reference book: Applied Cryptography, Bruce Schneier

Course Objectives
This course covers the usage of cryptographic protocols for computer and network applications. Assuring the quality, validity and privacy of information is one of the key applications of Cryptography. Applications of cryptography ranges from signatures, certificates to trustless multiparty computations.

Course Outcomes:
After the course the student will be able to:

1. Understand the algorithms used for constructing cryptographic computations
2. Understand the concept and correctness of cryptographic protocols.
3. Understand the methods used for encryption, authentication, integrity, certification and data privacy.
4. Understand the complex protocols that involve many steps and computing agents, who do not trust each other.
5. Understand how seemingly impossible electronic transactions can be performed (e.g. digital cash).

Evaluation:
Students are assessed on grades received in projects, homeworks, exams. The grades are "curved" for determining grade cutoff points on an A, B, C scale. The weight distribution is Assignments: 30% Mid-Term Exam: 30% Final Exam: 40%.

There will be no make-up exams or extra credit assignments. None.

Important Things:

1. MCS "portfolio": Yes, the class projects are eligible for MCS portfolio.
2. Academic Dishonesty: You are responsible for understanding what consists academic dishonesty. No tolerance policy will be in effect and a grade of F or XE will be awarded and a report will be filed with Fulton School. Please refer to https://provost.asu.edu/files/AcademicIntegrityPolicyPDF.pdf for details -- also please note item N on Page 2.

Topics:
Computer Security

- Network and System Security

- Threat Models
- Vulnerabilities and Hacking

Cipher construction
- Symmetric Block and Stream Ciphers
- History of Cipher generation
- One Time pad and other ciphers

Cryptographic tools
- Random Numbers
- Hash Functions
- Symmetric Encryption (DES, AES)
- Asymmetric Encryption (RSA)

Password Storage and hacking
- Hashed password storage
- Attacks on Hashes
- Rainbow Tables
-

Asymmetric Encryption
- Merkle, Diffie-Helman
- Public Key Systems
- Key Exchange and Communication

Cryptographic Protocols
- Types of protocols
- Trust and computation
- Validating Cryptographic protocols and attacks
-

Digital Signatures and Certificates
- Digital Signatures
- Digital Certificates
- PKI and Certificate Authorities

SSL/TLS
- Secure communications on the web
-

The RSA cipher
- Number Theory
- Modulus and exponentiation
- The RSA property
- Factorization and Primality testing

More Cryptographic Protocols
- Timestamping Protocols
- Blind Signatures
- Secret Splitting and Sharing
- Signature Schemes
- Zero Knowledge Proofs
- Cut and Choose

Advanced Crypto Protocols

- Secure Election Protocols
- Secure Digital Cash

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at https://sexualviolenceprevention.asu.edu/faqs.

As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, https://eoss.asu.edu/counseling, is available if you wish discuss any concerns confidentially and privately.