CRYPTOGRAPHY

EECS 480G

COURSE DESCRIPTION: This course begins with a discussion of how mobility-driven computing and communication systems use cryptography to protect data and protocols. The foundation for critical cryptographic concepts, techniques, and algorithms are covered. The fundamental cryptographic concepts are studied, including: symmetric encryption, public key encryption, digital signatures, cryptographic hash function, and message authentication codes; cryptographic protocols, such as key exchange, remote user authentication, and interactive proofs; cryptanalysis of cryptographic primitives and protocols, such as by side-channel attacks, differential cryptanalysis, or replay attacks; and analytic techniques on deployed systems, such as memory remanence, timing attacks, fault attacks, and differential power analysis. Techniques used for code making (cryptographic) and break codes (cryptanalytic) are covered, as well as how these techniques are used within larger security systems.

(3 credit hours)

FACULTY: To be announced


COURSE OBJECTIVES: This course is designed to provide a strong foundation in cryptography.

COURSE GRADE:

Exams (30%): 3 Exams, 1 every 3-4 weeks
Homework (40%): 4 assignment, ~ biweekly
Project (30%): Building on the homework to integrate and instill the learning experience.

WEEKLY COURSE SCHEDULE:
1. Introduction Cryptography
2. Classical Encryption Techniques
3. Block Ciphers and the Data Encryption Standard
4. Finite Fields I: Groups, Rings, and Fields
5. Finite Fields II: Modular Arithmetic
6. Finite Fields III: Polynomial Arithmetic
7. Finite Fields IV: Finite Fields of the Form GF(2^n)
8. AES: The Advanced Encryption Standard
9. Using Block and Stream Ciphers for Secure Wired and WiFi Communications
10. Key Distribution for Symmetric Key Cryptography and Generating Random Numbers
11. Prime Numbers and Discrete Logarithms
12. Public-Key Cryptography and the RSA Algorithm
13. Certificates, Certificate Authorities, and Digital Signatures
14. Elliptic Curve Cryptography and Digital Rights Management
15. Cryptoanalysis

University Student Ethics Policy
http://studentaffairs.case.edu/ai/policy.html
Violations of the Student Ethics Policy will result in failure in the assignment in question or the course, or referral to the academic integrity board as per university policy.

All forms of academic dishonesty including cheating, plagiarism, misrepresentation, and obstruction are violations of academic integrity standards. Cheating includes copying from another's work, falsifying problem solutions or laboratory reports, or using unauthorized sources, notes, or computer programs. Plagiarism includes the presentation, without proper attribution, of another's words or ideas from printed or electronic sources. It is also plagiarism to submit, without the instructor's consent, an assignment in one class previously submitted in another. Misrepresentation includes forgery of official academic documents, the presentation of altered or falsified documents or testimony to a university office or official, taking an exam for another student, or lying about personal circumstances to postpone tests or assignments. Obstruction occurs when a student engages in unreasonable conduct that interferes with another's ability to conduct scholarly activity. Destroying a student's computer file, stealing a student's notebook, and stealing a book on reserve in the library are examples of obstruction.