ICS 555 - DATA SECURTY & CRYPTOGRAPHY

Sections: 01

Term: 242

INSTRUCTOR: Sultan Almuhammadi
OFFICE: 22-316
PHONE: 860-1625
E-MAIL: *sultan* (@*almuhammadi.com*)

COURSE SITE: *www.almuhammadi.com/sultan/ics555* (see also *Blackboard, MS Teams*)

COURSE DESCRIPTION

Mathematical principles of cryptography and data security. A detailed study of conventional and modern cryptosystems. Zero knowledge protocols. Information theory, Number theory, complexity theory concepts and their applications to cryptography.

PREREQUISITES ICS 353 (ICS 454 is very recommended)

COURSE OBJECTIVES

1. To introduce the students to basic number theory concepts and algorithms related to cryptography.
2. To study variety of existing crypto-systems and develop problem-solving skills for cryptographic problems and applications.

COURSE LEARNING OUTCOMES

After completion of this course, the student should be able to:

1. explain basic concepts in number theory and apply modular arithmetic in problem-solving
2. understand foundational knowledge of group theory
3. understand the setups, the protocols, and the security issues of some existing cryptosystems
4. examine the security of a given cryptosystem

EVALUATION

Coursework: - attendance and class participation - in-class and online activities - homework/programming assignments - quizzes and take-home quizzes	25 %
Term Paper/Project	20 %
Midterm Exam	25 %
Final Exam	30 %

TEXTBOOKS AND REFERENCES

1. B. Forouzan, Cryptography and Network Security, 2008.
2. N. Koblitz, A Course in Number Theory and Cryptography, (2^{nd} edition, 1994)
3. W. Stallings, "Cryptography and Network Security," 7Th Edition, 2018
4. M. Bellare and P. Rogaway, Introduction to Modern Cryptography
5. A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography
6. B. Schneier, Applied Cryptography, (2^{nd} edition, 1996)

CONTENTS

The following schedule is tentative and subjected to changes. More details will be announced in the class and course website/Blackboard.

1. Introduction to Number Theory, Modular Arithmetic, Complexity theory.
2. Group Theory, Finite Fields and Quadratic Residues.
3. Cryptography, Cryptanalysis, and Perfect secrecy.
4. Symmetric key cipher, Block cipher.
5. Public key cipher: RSA, Diffie-Hellman, Massey-Omura, ElGamal, and Rabin's Cryptosystems.
6. Secure hashing, Authentication, Digital signatures (DSS).
7. Zero-Knowledge Proofs and Oblivious Transfer.
8. Elliptic-curve cryptography.
9. Blockchain and cryptographic applications.

NOTES

1. Coursework includes participation, online and in-class discussions, attendance, homework assignments and quizzes. Active learning is implemented in this class. Students are expected to be positively engaged in the learning process.
2. Regular attendance will be maintained during this course. Exceeding six absences will result in a DN grade.
3. Unexcused absences may reduce your coursework score. If you find yourself unable to attend a class for some reason, you should email the instructor ahead of time (at least 12 hours before the class). If you fail to do so, send your email as soon as you get a chance (even after the class) and explain your excuses if any.
4. No makeup homework, quizzes or exams would be given.
5. Late assignments are subjected to late penalty. See late submission policy on course website under the Assignments page.