CSS 527 Foundations and Applications of Cryptography

This course explores the foundations and applications of cryptography. The course covers randomness and set theory in the context of building cryptographic algorithms. The course covers cryptographic protocols, hashing, digital signatures, public key infrastructure and the trade-offs involved with each cryptographic technique. The course explores the application of cryptography to systems such as cloud computing, blockchain, and anonymizers. Political, social, and economic issues are discussed.

Learning Objectives

- Describe the mathematical foundations of cryptographic algorithms such as DES, AES, RSA, Diffie-Hellman, and SHA-256.
- Describe the use of cryptographic primitives to create secure systems.
- Define and correctly implement cryptographic algorithms for the protection of information at rest and in transit.
- Describe the life cycle issues associated with cryptographic materials, such as keys, and identify appropriate control measures for each part of the life cycle.
- Describe the human factors that impact secure use, administration, maintenance of, and disposal of cryptographic elements in a software system.
- Name, define, and describe common attacks on cryptographically secured information.
- Describe how cryptography can support the security requirements of a software system and describe where cryptography is inappropriate.

Grading

Homework	20.00%
Projects	15.00%
Research	15.00%
Quizzes and Exams	50.00%

Homework, Research and Projects

Assignment 1 is designed to give the student hands on experience performing encryption and decryption.
Assignment 2 is designed to give the student hands on experience performing hashing functions.
The **research assignment** is designed to give the student an opportunity to explore the state of the art in an area of interest related to cryptography, but not specifically taught in this class.
The **final project** will be similar to the assignments, but it will provide the student with an opportunity to work on applications and implementations of cryptographic libraries.

Exams

The class will have **one exam**. The exams will be primarily short answer questions related to the terminology, concepts, and practices covered in the class. It will cover all material from the course. A study guide will be provided on the canvas website.

There will be regular 10-15 minute **quizzes** during this class. They will generally be once a week and cover the lecture and outside reading for the class from the previous week. There will be approximately 8-10 quizzes depending on the rate at which material is covered. Generally expect these will occur on Wednesdays at the beginning of class, but I will announce any changes to this schedule.

Required Textbooks

- Readings will be required on a weekly basis from freely available academic literature

Recommended Textbooks and Readings

- Douglas R. Stinson, *Cryptography: Theory and Practice*.
- Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*.
- Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*.
- Bruce Schneier, *Applied Cryptography*.

Tentative Schedule

Week 0
Course overview. Symmetric cryptography. Security of symmetric cryptography. Block ciphers.
Week 1
Randomness. Building and using block ciphers. DES.
Week 2
Finite Mathematics
Week 3
AES. Stream ciphers.
Week 4
Public-key cryptography. RSA. Diffie-Hellman key exchange. ElGamal key agreement.
Week 5
Digital signatures. Cryptographic Hashing. HMAC.
Week 6
Elliptic Curve Cryptography. Homomorphic Cryptography.
Week 7
Public key infrastructure. X.509. PGP. Policy. Certificate management. SSL. S/MIME.
Week 8
Cryptographic Foundations of Blockchains.
Week 9
TOR. Electronic Voting. Cryptography in Cloud Computing.

Week 10
Quantum Cryptography. Social, Political, and Economic aspects of Security (Or why real security is hard)