CSE 4392, Special Topics: Applied Cryptography

Trevor Bakker, CISSP-IASSP, CISSP, CEH
trevor.bakker@uta.edu

December 1, 2023

The proposed undergraduate course on cryptography is essential in addressing the escalating demand for specialized knowledge in securing digital communication and information systems. While existing courses touch on cybersecurity, none delve into cryptography's intricacies and knowledge needed to evaluate and implement secure solutions, leaving a significant gap in our curriculum.

This course distinguishes itself by offering a focused exploration of cryptographic fundamentals, including mathematical foundations, security models, and real-world applications. Unlike broader information security courses, it provides in-depth coverage of topics such as symmetric and public-key encryption, block and stream ciphers, elliptic curve encryption, as well as post-quantum cryptography, homomorphic encryption—areas crucial for understanding contemporary cybersecurity challenges. Given the breadth of CSE 4380 and CSE 4381 only a cursory coverage of cryptography is provided during a semester.

Students will gain practical experience in using and analyzing multiple cryptographic algorithms. This dedicated course ensures that graduates possess a nuanced understanding of cryptography, making them adept at addressing emerging threats and contributing meaningfully to the field of cybersecurity.

This course will be offered in the Computer Science degree program. The proposed course would qualify as a technical elective.

Student Learning Outcomes

Upon completion of this course the student will be able to understand and explain:

1. The mathematical background of cryptography.
2. The concepts used in early substitution and translation ciphers.
3. The differences between and implications of random and pseudo-random numbers
4. Block ciphers and some classic block-cipher constructions (DES, 3DES and AES).

5. Stream ciphers such as RC4, ChaCha, and Salsa20
6. Message allocation such as MAC, HMAC, GCM
7. Public-key cryptography including RSA functions and the other based on the Diffie-Hellman protocol.
8. Elliptic curve cryptography such as ECDH, ECDSA and ECMQV
9. Post-quantum cryptography including Kyber and Dillithium.

   Upon completion of this course the student will also be able to:

10. Demonstrate the ability to analyze a complex privacy / security problem and design and implement a strong cryptographic solution using symmetric key and public key encryption

Attachments

1. Sample course syllabus and course schedule
2. Sample course homework assignment