CSCE 5050 Applications of Cryptography (Summer 2022)

Instructor: Abdelnasser Ouda CSCE , email: abdelnasser.ouda@unt.edu, room NTDP F203
Office Hours: 5050-003 Thursdays 12-1:30 PM 
5050-004 Thursdays 1:30-3:00 PM
TA 5050-003: Md Marufi Rahman, CSCE, email: mdmarufirahman@my.unt.edu
TA 5050-004: Syed Badruddoja, CSCE, email: syedbadruddoja@my.unt.edu

Course description: This course aims at introducing fundamentals of cryptography and their applications. The knowledge gained from this course will enable students to apply cryptographic algorithms as building blocks for designing secure solutions.

Course Lectures & Topics
- Course overview, historical ciphers, mathematical background
- One-time pad, stream ciphers and pseudorandom generators
- Block ciphers & Block cipher modes of operation
- Data integrity and message authentication codes (MACs)
- Data integrity and cryptographic hash functions & Authenticated encryption
- Overview of key exchange, public-key encryption, and their mathematical background Plus more in Public-key encryption
- Digital signatures and identification schemes
- Public-key infrastructure, authenticated key exchange, and TLS
- Identification protocols and secure login;
- Overview of quantum cryptanalysis and post-quantum cryptography
- Blockchain and cryptocurrencies
- Advanced cryptographic functionalities: homomorphic encryption, secret sharing, and secure multi-party computation; Review of the material covered in the course

Recommended literature:
- D. Boneh and V. Shoup: “A Graduate Course in Applied Cryptography”. Available as draft at: http://toc.cryptobook.us/
- M. Rosulek: “The Joy of Cryptography” Available as draft at: https://web.engr.oregonstate.edu/~rosulekm/crypto/

[Supplementary reading]:

Grading:
- 3 Assignments/Projects – 60%, 20% each
- Mid-term exam – 10% (Second week of June)
- Final exam – 30% (Second week of July)