ECE 628 - Computer Network Security  
Winter 2023  

Instructor:  Professor G. Gong  
Office: ggong@uwaterloo.ca  
https://uwaterloo.ca/scholar/ggong  
Office hours: TBA  

Course Description  
This course focuses on the fundamental principles of how to secure computer networks. The topics to be covered include applied cryptography, encryption, authentication, and zero-knowledge proofs, semantic security, network security, trusted platform, Decentralized system security, blockchain and cryptocurrency, data privacy enhanced technologies, secure machine learning, physical layer attacks, quantum key distribution,  

Background Requirements  
Students attending this course should have a good working knowledge of probability theory and computer networks.  

Resources  
Lectures: 01:00-3:50 Th, E5 5106  

References  
There is no textbook for the course, but the following references will be helpful for your reading.  


4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014 (you may read it if you wish to have a deep crypto knowledge for your future career, but not required from the course).  

5. Supplemental materials for the book by Chen-Gong.  

6. ECE 628 Course Notes -Available on UW-LEARN.  

7. Selected papers.  

Course Grading  
The overall grade is based on a midterm exam (take-home exam), one project and one final exam.  

Course Project  
A list of project problems will be given, however students are encouraged to propose their interested problems related to the course materials which should be discussed with the instructor for approval.
Course Outline

1. Introduction to Cryptology: cryptography and cryptanalysis, confidentiality, integrity and authentication, digital signatures, active and passive attacks, and classification of cryptographic systems.


5. Network Security: the man-in-the-middle attacks, mutual authentication and key establishment, cipher suite negotiation, network security protocols (IPsec, TLS/SSL, VPN), Web security (https), and attacks on TLS

6. Wireless security: radio air link protection (4G-LTE, 5G), IEEE 802.11 security solutions (flowed WEP, CCMP), physical layer jamming and relay attacks on RFID challenge response.

7. Internet Authentication: hash chain, Merkle tree authentication, password based authentication, Kerberos, and PKI.


Other Resources

- A Graduate Course in Applied Cryptography in Stanford University: https://crypto.stanford.edu/~dabo. (From this site, you may download the text book, authored by Dan Boneh and Victor Shoup.)
