ECE 409 - Cryptography and System Security
Winter 2019

Instructor: Professor G. Gong

Office: EIT 4158, x35650, ggong@uwaterloo.ca

http://comsec.uwaterloo.ca

Office hours: TBA

Course Description: This course will provide introduction to cryptology and system security, theory of secure communications, points of attacks, symmetric-key and public-key cryptographic algorithms, network security protocols, access authentication, wireless system security, blockchain security, and applications.

Outcomes: Equip students with cryptography and security basics in modern computer network and systems.

Prereq Topics: Mathematical reasoning, discrete math, statistics, probability.

Prereqs: Level at least 4A Computer Engineering or Electrical Engineering or Software Engineering.

Antireqs: CS 458

Resources

Text: L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.

References:

1. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014.
2. ECE 409 Course Notes -Available on UW-LEARN.

Course Outline

1. Introduction to cryptography and system security: cryptology, cryptanalysis, classification of cryptosystems, and basic concepts of secure systems.
2. Networks, Systems and Finite Fields: Model of secure systems, types of attacks, attacking points, trust and threat models, trusted platform, and arithmetics of finite fields.
3. Security and Pseudorandomness: Perfect secrecy, pseudorandomness, computational security, semantic security, LFSR based pseudorandom generation, and correlation attacks.

4. Symmetric-key Cryptographic Systems: design principles, cipher systems (WG, AES, SHA, MAC), birthday attacks, and time-memory trade-off attacks.

5. Public-key Cryptographic Systems: arithmetic operations, discrete logarithm and integer factorization algorithms, learning with error, public-key systems (RSA, DH, DSS, ECC, and FHE), hashing chain authentication, and faulty attacks.

6. Implementing Secure Systems: infrastructure support, key generation, crypto specifications, PKI, X.509 certificates, and key escrow.

7. Network Security Protocols: the man-in-the-middle attacks, mutual authentication, key establishment, security association, network security protocols (IPsec, TLS), and attacks on TLS.

8. Access Authentication: basic concepts in access authentication, wireless access authentication and key agreement (AKA), AAA, and attacks on password based authentication.

9. Wireless System Security: air link protection (3G/4G-LTE), IEEE 802.11 security solutions (flawed WEP, CCMP), and jamming and location service attacks.

10. Applications and Special Topics: IoT, blockchain and cryptocurrency, and privacy preserving machine learning.

Tutorial Description: Question and answer on material covered in lectures and homework assignment, and problem solving skills.

Course Grading: The overall grade is based on two sets of assignment questions, one course project (individual or 2-person group), and one final exam. For the project, a list of the project problems will be provided. Program demo and a report of 5-10 pages is a must to obtain the score.

Other Resources

- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.

- BugTraq, http://www.securityfocus.com/archive/1. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.