ECE 409 - Cryptography and System Security
Winter 2016

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 computer security, theory of secure communications, points of attack, conventional cryptographic systems, public key cryptographic systems, network standards and protocols, wireless system security, and applications.

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

Prereq Topics: mathematical reasoning, combinatorics, statistics, probability.

Prereqs: ECE 358, or Level at least 4A Computer Engineering or Electrical Engineering or Software Engineering.

Antireqs: CO 485, 487, CS 458

Teaching Assistant: Yao Chen, y449chen@uwaterloo.ca, EIT-4165, x37476.

Resources

Lectures:	01:30-02:20MWF, RCH 209
Tutorials:	05:30-06:20M RCH 208
Text:	L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.
References:	- ECE 409 Course Notes -Available on UW-LEARN.
	- W. Stallings, Cryptography and Network Security: Principles and Practice, 6/E, Prentice Hall, 2014.

Course Outline

1. Introduction to cryptography and system security (notes): cryptology, cryptanalysis, encryption and authentication, classification of cryptosystems, and basic concepts of secure systems.
2. Networks, Systems and Finite Fields (chapter 1 and notes): Model of secure systems, types of attacks, attacking points, trust and threat models, trusted platform, and arithmetics of finite fields.
3. Conventional Cryptographic Systems (chapters 2-4, notes): Perfect secrecy, pseudorandomness, computational security, symmetric-key systems (A5, RC4, WG, DES, AES, SHA1, SHA3, MAC), correlation attack, birthday attacks, and time-memory trade-off attacks.

4. Introduction to Public Key Cryptographic Systems (chapter 5, notes): arithmetic operations, discrete logarithm and integer factorization algorithms, public-key systems (RSA, DH, DSS, ECC, LWE and FHE), faulty attacks on RSA.

5. Implementing Secure Systems (chapter 6, notes): infrastructure support, key generation, crypto specifications, PKI, X.509 certificates, and key escrow.

6. Internet Standards and Protocols (chapters 7-8, notes): the man-in-the-middle attacks, mutual authentication, key establishment, security association, network security protocols (IPsec, SSL/TLS, SSH, S/MIME), protection models, attacks on SSL/TLS, and firewalls.

7. Wireless System Security (chapters 9 and 10): wireless access authentication and key agreement, AAA, EAP, air link protection (3G/4G-LTE), IEEE 802.11 security solutions (flawed WEP, CCMP).

8. Applications (notes): IoT, RFID systems, smart cards, side-channel attacks, trusted platform module, cloud security, and image encryption.

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 assignment questions, one course project (individual), one midterm exam, and one final exam, which is distributed below.

		Due Dates
Assignment Questions	10%	February 1
Midterm Examination	30%	
Course Project	10%	March 21
Final Examination	50%	

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.