ECE 409 - Cryptography and System Security
Winter 2015

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 4132, ext. 32140.

Resources

Lectures:	11:30-12:20MWF, RCH 109
Tutorials:	03:30-04:20F, RCH 209
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.

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

Course Outline

1. Introduction to cryptography and system security (notes): cryptology, cryptanalysis, encryption and authentication, classification of cryptosystems, and basic concepts of secure communications.

2. Networks and Systems (chapter 1): Model of secure systems, types of attacks, attacking points, trust model, threat model, trusted platform, and protected communications.

3. Conventional Cryptographic Systems (chapters 2-4, notes): Randomness measurements, pseudo-random sequence/number generators, stream ciphers, block ciphers, encryption models, secure hash functions, MAC, correlation attack, birthday attacks, and time-memory trade-off attacks.

4. Introduction to Public Key Cryptographic Systems (chapter 5): arithmetic operations, RSA, DH, DSS, ECC, and FHE.

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, LTS/SSL, SSH, S/MIME), protection models, 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), and jamming attacks.

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

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 6
Midterm Examination	30%	February 25
Course Project	10%	March 30
Final Examination	50%	