ECE 710 Topic 21
Communication Security, Spring 2016

Instructor: Professor G. Gong
Office: EIT 4158, x35650, ggong@uwaterloo.ca
http://comsecuwaterloo.ca/∼ggong
Office hours: by appointment

Time: 02:30-05:20F

Room: EIT 3141

Course Outline: This course introduces some timely topics in communications security. It covers the advanced topics on cryptography, encryption and authentication, homomorphic encryption, cryptanalysis, provable security, network security mechanisms and protocols, network access authentication, radio air link protection, privacy in radio frequency identification systems, game theory and security in wireless spectrum sharing, attacks, and hardware protections.

Prerequisites: ECE 409 or ECE 458, or equivalent courses taken from other departments or universities.

References:

1. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012. Chapters 2-3, 6-10.
2. L. Buttyàn and J.P. Hubaux, *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behaviour in the Age of Ubiquitous Computing*, New York, Cambridge University Press, 2008 (TK5102.85 .B88). Chapters 8 and 11.
3. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC, 2007.
4. Some notes and supplement materials will be provided.

Course Outline

1. Introduction to cryptology: cryptography and cryptanalysis, information security, confidentiality, integrity and authentication, and digital signatures, wiretapping, active and passive attacks, requirements on secure systems, classification of cryptosystems.
2. Security metrics of communication systems: perfect forward secrecy, computational complexity, and provable security.
3. Symmetric-key systems: arithmetics of finite fields, pseudo-random sequence generators, randomness criteria, correlation attacks, stream ciphers, block ciphers, secure hash functions, MAC, and time-memory trade-off attacks.

4. Public-key systems: modular arithmetic, CRT, factorization of big integers, discrete logarithms, digital signatures, homomorphic encryption, and fault attacks.
5. Security infrastructure: infrastructure support, key generation, crypto specifications, PKI, X.509 certificates, and key escrow.
6. Network security protocols: the man-in-the-middle attacks, mutual authentication, key establishment, security association, Internet security protocols (IPsec, MAPsec, SSL/TLS), end-to-end/hop-by-hop encryption, and attacks on SSL/TLS.
7. Network access authentication: authentication and key agreement (AKA) in cellular systems, AAA, and extensible authentication protocols (EAP), tunnelled attacks on EAP/TLS, and mobile multi-channel authentication.
8. Wireless network security: special aspects of wireless protection, radio air link protection, IEEE 802.11 security solutions, and forgery attacks on integrity and authentication.
9. Special topics: privacy model, privacy in RFID systems, location privacy in vehicular networks, game theoretic model and wireless spectrum sharing, anti-jamming attacks, hardware protection.

Course Grading: The overall grade is based on assignment questions, one project and one final exam, which is distributed below.

Assignment Questions:	20%
Project (individual):	30%
Final Examination (open book exam):	50%

Course Project: A list of project problems will be given, however students are allowed to suggest problems related to their own research which should be discussed with the instructor for approval.