# ECE 628 - Computer Network Security
# Winter 2019

**Instructor:** Professor G. Gong

Office: [redacted] x35650, ggong@uwaterloo.ca

http://comsec.uwaterloo.ca

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 and authentication, semantic security, attack analysis, network security protocols, wireless security, implementations and side-channel attacks, trusted platform, advanced cryptographic algorithms, and applications of IoT, blockchain, and privacy preserving machining learning.

## Background Requirements

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

## References

(a) L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.

(b) J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014.

(c) ECE 628 Course Notes -Available on UW-LEARN.

(d) Selected papers.

## Course Outline

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

2. Networks, Systems and Randomness: points of attacks, secure infrastructure, trust and threat model, Shannon's secrecy, complexity theory, semantic security, pseudorandom generatorors, randomness criteria, and correlation attacks.

3. Symmetric-key Systems: Stream ciphers and block ciphers, lightweight cryptography, encryption models, chosen plaintext/ciphertext attack, secure hash functions and MAC, authenticated encryption, and time-memory trade-off attacks.

4. Finite Field Arithmetic: modular arithmetic, finite fields, Euclid's GCD, primality test, CRT, factorization of big integers, discrete logarithms, and learning with error.

5. Public-key Systems: security of public-key cryptography, basic schemes, ECC, pairing-based IBC, fully homomorphic encryption and fault attacks.

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

7. Access Authentication: authentication and key agreement (AKA) in cellular systems, AAA, password based authentication, Kerberos, Open-authorization, extensible authentication protocols (EAP), and tunnelled attacks on EAP/TLS.

8. Wireless Security: radio air link protection (4G-LTE), IEEE 802.11 security solutions (flowed WEP, CCMP), jamming and location service attacks.

9. Advanced Cryptographic Algorithms: secret sharing, multiparty computation, commitment schemes, and zero knowledge proof systems.

10. Implementations and Trusted Platform: smart cards, side-channel attacks, root of trust, secure boot, validation and authorization, secure storage, trusted platform module, and SGX.

11. Applications: Internet-of-Things (IoT), near field communication (NFC) and replay attacks, blockchain and cryptocurrency, and privacy preserving machine learning.

**Course Grading**

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

| | |
|---|---|
| Assignment Questions | 25% |
| Project (individual) | 25% |
| 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.

- A Graduate Course in Applied Cryptography in Stanford University: `https://crypto.stanford.edu/~dabo`