ECE628 Computer Network Security
Winter 2022

Instructor:

G.B. Agnew, [redacted] X33041, gbagnew@uwaterloo.ca

References:

- E&CE628 Course Notes – Available online
- Selected Papers

Lectures:

[redacted]

Description:

This course will deal with many aspects of Cryptography, Cryptanalysis, Data and Communications Security.

Topics will include:

- Introduction to cryptography, secrecy, authentication and digital signatures
- The theory of secure communications
- Study of conventional and public key cryptographic systems
- Cryptanalysis of cryptographic systems
- Protocol development and analysis
- Implementations of secure systems
- Timing and Power Attacks
- Wireless System Security
- Applications such as Blockchain technology

Grading:

There will be a series (4) of quizzes that will involve testing of knowledge of assigned papers, videos and the course material. – 40%

There will be a major final project/paper – 60%

Background Requirements

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

ECE628 Computer Network Security
Course Outline

1. Introduction to Cryptology

- cryptography, cryptanalysis
- security, authentication, digital signatures
- wiretapping, active and passive
- secure system requirements
- classification of cryptosystems

2. Theory of Secure Communications

- Shannon theory for secure systems
- entropy
- equivocation
- redundancy
- random cipher model
- unicity distance
- complexity theory
- cryptographic classifications of security

3. Networks and Systems

- applications of cryptography
- points of attack
- security issues
- link/end-to-end encryption

4. Conventional Cryptographic Systems

- principles of confusion and diffusion
- Block Ciphers/Stream Ciphers
- simple transposition ciphers
- substitution ciphers
- homophonic substitution
- Beale Ciphers
- polyalphabetic substitution
- Vigenere cipher
- Beaufort cipher
- index of coincidence
- Kasiski method
- running key ciphers
- Rotor machines
- product ciphers
- Strict Avalanche Condition
- Lucifer cipher

- Feistel Ciphers
- DES
- IDEA
- AES
- cryptanalysis
- MD5
- SHA -1, SHA-2, SHA-3
- Key Management

5. Finite Field Arithmetic

- modular arithmetic
- Euclid's GCD
- Primality
- finite fields and extension fields
- CRT
- Factoring
- Logarithms
- Number Representations

6. Public Key Systems

- RSA
- D-H
- Elliptic Curves
- Zero Knowledge systems

7. Protocols and Applications

- PKI
- Threshold Schemes
- Suite B Algorithms
- Standards (P1363, FIPS 140)
- Internet Security (IPSec, SSL, TLS, S/MIME)
- Firewalls
- Wireless Systems and security (WiFi, Bluetooth, etc.)
- Blockchains

8. Implementations and Applications

- Smart Cards – characteristics and attacks
- Power Attacks and Timing Attacks
- Copyright protection and Electronic Watermarks
- Digital Rights Management

Academic integrity, Grievance, Discipline, Appeals and Note for students with disabilities:
See http://www.uwaterloo.ca/accountability/documents/courseoutlinestmts.pdf
The text for this website is listed below:
Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check www.uwaterloo.ca/academicintegrity/ for more information.]
Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4, http://www.adm.uwaterloo.ca/infosec/Policies/policy70.htm. When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.
Discipline: A student is expected to know what constitutes academic integrity to avoid committing academic offenses and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offense, or who needs help in learning how to avoid offenses (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course professor, academic advisor, or the undergraduate associate dean. For information on categories of offenses and types of penalties, students should refer to Policy 71, Student Discipline, http://www.adm.uwaterloo.ca/infosec/Policies/policy71.htm. For typical penalties check Guidelines for the Assessment of Penalties, http://www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm.
Appeals: A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72, Student Appeals, http://www.adm.uwaterloo.ca/infosec/Policies/policy72.htm.
Note for students with disabilities: The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with the OPD at the beginning of each academic term.