Syllabus for CMPT 404 - Cryptography and Protocols

Instructors

Name: David Lindberg

Email: dll4@sfu.ca

Office Hours: Tu 13:00–15:00 (starting from Jan 17th) in TASC 8013, or by appointment

Office Location: TASC II 8013

Name: Kevin Mann

Email: kma50@sfu.ca

Office Hours: Tu 13:00–15:00 (starting from Jan 17th) in TASC 8013, or by appointment

Office Location: TASC II 8013

Teaching Assistants

Name: Marcus Naslund

Email: mnaslund@sfu.ca

Office Hours: TBD

Office Location: ASB

Name: Allison Ng

Email: allisonn@sfu.ca

Office Hours: TBD

Office Location: ASB

Name: Derek Fong

Email: drf1@sfu.ca

Office Hours: TBD

Office Location: ASB

Name: Sean Maloney

Email: seanm@sfu.ca

Office Hours: TBD

Office Location: ASB

Class Information

Lecture Time:

Tu 10:30–11:20, in SWH 10051 Th 9:30–11:20, in SWH 10051

Prerequisites:

MACM 201, some knowledge of probability and complexity is helpful, although not necessary.

Books:

Cryptography and network security. Principles and practice, by William Stallings, Pearson, 2003: 3rd edition
Introduction to modern cryptography, by Jonathan Katz, Yehuda Lindell, Chapman and Hall, 2008
Handbook of Applied Cryptography, by lfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanston, CRC-Press, 1996
Practical cryptography, Niels Ferguson, Bruce Schneier, Wiley Publishing, 2003

Topics:

■Basics of probability, cryptography, and complexity. Historical remarks
■Concepts of privacy and authenticity: perfect, statistical, and computational
■Pseudo-random generators and functions
■One-way functions
■Private-key encryption: constructions, block ciphers
■Trapdoor functions and public-key encryption
■Message authentication, digital signatures, and hashing
■Zero-knowledge proofs
■Electronic auctions, voting etc.
■Cryptographic components of the existing protocols

Marking Scheme:

44% Final
32% Assignments (4 of them)
24% Quizzes (3 of them)

Academic Honesty:

Academic Honesty plays a key role in our efforts to maintain a high standard of
academic excellence and integrity. Students are advised that ALL acts of intellectual dishonesty are subject to disciplinary action by the School; serious infractions are dealt with in accordance with the Code of Academic Honesty (T10.02 (http://www.sfu.ca/policies/teaching/t10-02.htm). Students are encouraged to read the School's Statement on Intellectual Honesty (http://www.cs.sfu.ca/dean-gradstudies/honesty.html).

Created: March 27, 2012, 12:26 a.m.
Last Updated: April 6, 2012, 9:36 p.m.