CPSC 418/MATH 318 — Final Exam Study Guide

Exam logistics

- Date and time: Monday December 13, 15:30-18:30 in SB 103 (our regular lecturer room)
- What to bring: pen/pencil and eraser, refreshment (e.g. water bottle, soft drink, coffee), mask
- What not to bring: paper, notes, phone, tablet, laptop (bags and backpacks can be stored at the front of the room)

General remarks

- CPSC 418 and MATH 318 will have identical final exams.
- No aids will be allowed; this includes notes, books, handouts, internet access, calculators etc.
- You will be examined on all the material of the course, including the material that was tested on the midterm exam (Weeks 1-8), but with substantially more emphasis on material not tested on the midterm exam (Weeks 9-13). The material that you will be examined on is described in detail below.
- It is important to know *concepts*, not just details.

Exam format

- Questions asking you to state a definition or theorem
- Short answer questions — multiple choice, yes/no, 1-3 word answers
- Semi-short answer questions — answer plus a brief explanation
- Longer answer question — answer plus a somewhat longer explanation (e.g. a short paragraph)
- Mathematical questions — may require a short proof or mathematical verification

Material covered

- The material on the midterm study guide
- Public key cryptosystems
  - Trapdoor one way functions
  - Definition and ingredients of a public key cryptosystem, services provided by public key cryptography
  - RSA, security of "textbook" RSA: equivalence of factoring n, computing $\phi(n)$ and finding d, choice of secure parameters
  - Multiplicative attacks on "textbook" RSA (CCA, meet-in-the-middle), basic idea of RSA-OAEP (no details) and why/how it fixes problems of "textbook" RSA
  - Randomized encryption — you should be able to work with ElGamal key generation, encryption and decryption procedures, but you need not remember the details. You don't need to know the details of the Goldwasser-Micali PKC.
  - Facts and security assumptions for ElGamal and Goldwasser-Micali
- Formal Notions of security for public key cryptosystems
  - Security against passive attacks: polynomial/IND-CPA and semantic security

  - Security against active attacks: IND-CCA2 security, non-malleability, plaintext awareness and how they relate to each other logically

- Signatures
  - Definition, of properties of, and services provided by digital signatures
  - Signatures from PKCs, impersonation attack on "textbook" PKC-based signatures and how to prevent this attack by using a cryptographic hash function
  - El Gamal signature scheme — you should be able to work with ElGamal key generation, encryption and decryption procedures, but you need not remember the details
  - Security assumptions for El Gamal
  - Notions of universal, selective and existential forgery
  - Definition of GMR-security

- Pseudorandom number/bit generation
  - Definition of a PRNG/PRBG, idea of a seed
  - Definition of cryptographically secure PRGB, next-bit test
  - Entropy and proper use of PRNGs

- Key management
  - Basic idea of symmetric key distribution via key distribution centres
  - Basic ideas of public key distribution by means of public key infrastructures; notions of certificates, certification authorities and their purpose

- Entity authentication
  - Services provided by entity authentication protocols
  - Station-to-Station protocol — you need not remember details, but you should know its purpose, what cryptographic services it provides, and that it is an authenticated version of Diffie-Hellman

- Cryptographic application
  - SSH — you need not remember details, but you should know what it is, its purpose, what cryptographic services it provides, and the basic three-layer structure

- Number theory
  - The number theory topics listed on the midterm study guide
  - Euler's and Fermat's Theorems, primitive roots
  - Euclidean algorithm and extended Euclidean algorithm, modular inverses, solving linear Diophantine equations and linear congruences
  - Binary exponentiation
  - Quadratic residues and non-residues, Euler's criterion
  - Legendre and Jacobi symbols and their properties, efficient computation of Legendre and Jacobi symbols, the Quadratic Residuosity Problem

* * * Happy Studying! * * *