UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics
Department of Computer Science

Mathematics 318 / Computer Science 418 Introduction to Cryptography

(see Course Descriptions under the year applicable: http://www.ucalgary.ca/pubs/calendar/)

Syllabus

Topics	**Number of Hours**
Symmetric Cryptography: *Overview*: What is cryptography? What services does it provide? What are its limitations? Attack models and types of attacks.	3
Symmetric Key Cryptography: Symmetric key cryptosystems. Classical ciphers. Information theory, one-time pad. Block ciphers, Advanced Encryption Standard, cryptanalysis of block ciphers. Modes of operation. Stream ciphers.	12
Data Integrity: Hash functions. Message authentication codes. Attacks on hash functions and MAC's.	4
Public-Key Cryptography: *Public Key Cryptography*: Number theoretic background. Key exchange problem, Diffie-Hellman protocol and attacks on Diffie-Hellman. Public-key cryptosystems, RSA and attacks on RSA.	5
Provable Security: Probabilistic encryption, ElGamal cryptosystem. Quadratic residues and the Quadratic Residue Problem. Security under passive attacks, semantic security. Goldwasser-Micali cryptosystem. Security under active attacks (IND-CCA2, non-malleability, plaintext awareness). RSA-OAEP.	3
Digital Signatures and Authentication: Signature schemes. Signatures from public-key cryptosystems. Security of signatures. ElGamal signature scheme and attacks,	2
Cryptography in Practice: Cryptographically secure pseudorandom bit generation. Key management, key hierarchies and pre-distribution (Kerberos), Public-key infrastructures and certification authorities. Entity authentication, authenticated key exchange (station-to-station protocol).	3
Applications: Email security via PGP. Access control via SSH.	1
Special Topics (time permitting); Brief overview -- Elliptic curve cryptography, Quantum cryptography, Quantum computing and post-quantum cryptography.	2
TOTAL:	**35**

Course Outcomes

The main objective of this course is to provide students with a thorough understanding of the fundamentals of and current best practices in cryptography. Students will have a solid understanding, including practical experience, of the basic cryptographic primitives and their proper usage. Illustrative real world examples of cryptographic systems are used to demonstrate how crypto- graphic primitives can be combined to provide robust security assurances. In particular, a student who successfully completes this course will be able to:

1. describe the different services that cryptography provides and give examples of cryptographic mechanisms that provide a given service.
2. verify that a cryptographic mechanism works properly, eg. that encryption followed by decryption is successful.
3. describe the different attack models covered in the course and how they relate to each other.
4. demonstrate competence with mathematical foundations of modern cryptographic primitives.
5. apply mathematics to assess the security of cryptographic primitives.
6. restate the main cryptographic protocols that are covered in the course and their different functions

In addition, students taking CPSC 418 will be able to

7. write software that provides cryptographic services and integrate existing cryptographic soft- ware libraries and packages in this software.

In addition, students taking MATH 318 will be able to

8. use mathematical reasoning to rigorously prove security properties of various cryptographic primitives.

* * * * * * *

2016:08:11
JM

2018:08:15
RS