UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

Pure Mathematics 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, shamir's secret sharing scheme. Block ciphers (DES, 3DES, AES), cryptanalysis of block ciphers. Modes of operation. Stream ciphers.	14
Data Integrity: Hash functions. Message authentication codes. Attacks on hash functions and MAC's.	3
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.	6
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.	4
Digital Signatures and Authentication: Signature schemes. Signatures from public-key cryptosystems. Security of signatures. ElGamal signature scheme and attacks, Digital Signature Standard. Entity authentication, authenticated key exchange (station-to-station protocol).	3
Cryptography in Practice:	
Key Management: Cryptographically secure pseudorandom bit generaton. Key hierarchies and pre-distrbution (Kerberos). Public-key infrastructures and certification authorities.	1
Cryptography in Practice: Email security and PGP. Access control and SSH.	1
TOTAL:	**35**

2012:09:01 Effective: Fall 2012
RS:jml