

FACULTY OF SCIENCE Department of Mathematics and Statistics

Pure Mathematics 669

Cryptography

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

Syllabus

<u>Topics</u>	Number of Hours
Symmetric Cryptography: Substitution Ciphers and Information Theory: What is cryptography? What services does it provide? What are its limitations? Symmetric cryptosystems, substitution and transposition ciphers. Entropy and perfect security, one-time pad. Redundancy, unicity distance.	<u>110015</u> 5
Block Ciphers: Block ciphers. Product ciphers, overview of DES and 3-DES, AES. Attacks on block ciphers. Modes of operation.	5
Public-key Cryptography: Number theory and Algorithms 1: Modular arithmetic, modular inverses. Binary exponentiation. Euler's φ-function. Chinese remainder theorem. Primitive roots.	3
Public-key Cryptography: One-way functions, Diffie-Hellman key exchange. One-way trapdoor functions and public-key cryptography, RSA, security of RSA.	3
Number Theory and Algorithms 2: Quadratic residuosity problem. Computing square roots modulo n.	2
Provably Secure Public-key Cryptography: Randomized public key cryptography, El Gamal public key system. Semantic security, Goldwasser-Micali system. Provable security, IND-CCA2, nonmalleability. RSA-OAEP.	4
Data Integrity and Digital Signatures: Hash functions and message authentication codes. Digital signatures, security of digital signatures. El Gamal signature scheme, Digital Signature Algorithm.	4
Elliptic Curve Cryptography: Elliptic curve group law, security of elliptic curve systems. ECMQV key agreement protocol.	3
Cryptography in Practice: Key Management. Cryptographically secure pseudorandom number generation. Key hierarchies and pre-distribution. Public-key infrastructures and certification authorities.	6
Cryptography in Practice: Email security and PGP. Access control and SSH.	2
Student Presentations:	4
TOTAL:	37

* * * * * *

2010:08:13 Effective: Fall 2010

RS:jml

Description change: 2011:07:01 WEC