Faculty of Mathematics
Department of Combinatorics & Optimization

C&O 685
The Mathematics of Public-Key Cryptography
Fall 2000 Course Outline

Instructor:	Douglas Stinson, MC 4028
Time:	11:30 - 12:45 TR
Location:	DWE 1501
Texts:	Cryptography: Theory and Practice (Stinson)
Additional Material:	Handbook of Applied Cryptography (Menezes, van Oorschot, Vanstone); available to be downloaded from the internet
Prerequisite:	PMATH 334, Introduction to Rings and Fields (or equivalent)
Calendar Description:	An in-depth study of public-key cryptography. Number-theoretic problems: prime generation, integer factorization, discrete logarithms. Public-key encryption, digital signatures, key establishment, secret sharing. Security definitions and proofs.

Lecture Topics:

Introduction
- Goals of cryptography
- Adversarial models
- Provable security

Algorithmic Number Theory
- One-way functions
- Prime generation
- Integer factorization
- Discrete logarithm problem
- Elliptic curve discrete logarithm problem
- Deffie-Hellman problem

Public-Key Encryption
- RSA
- ElGamal and derivatives
- Security proofs

Key Establishment
- Symmetric-key techniques
- Secret sharing schemes
- Public-key techniques
- Security proofs