UNIVERSITY OF
CALGARY

MEMO

FACULTY OF SCIENCE

Mathematics and Statistics

Telephone: (403) 220-5203
Fax: (403) 282-5150
www.math.ucalgary.ca

To: **STUDENTS INTERESTED IN CRYPTOGRAPHY** **Date:** November 8, 2001

From: Hugh Williams, I-core Chair
Department of Mathematics and Statistics

Re: **PMAT 603.38 -- PUBLIC-KEY CRYPTOGRAPHY**

The Department of Mathematics and Statistics is offering a graduate-level course in Public Key Cryptography for the Winter 2002 Semester -- PMAT 603.38. This course has been timetabled and interested students should register as soon as possible. Check the bulletin board outside MS 464 during the first week of January (Block Week) for the initial meeting time for this course. A regular course schedule will be decided at this meeting.

COURSE OUTLINE:

PMAT 603.38 PUBLIC-KEY CRYPTOGRAPHY

Prerequisites: PMAT 321 or consent of department.

Instructor: H.C. Williams, MS 360, Ph. 220-6322

Textbook: None.
Material will come from notes, handouts and published papers. The books *Public-Key Cryptography* by Arto Salomaa Springer Verlag, 1990) and *Handbook of Applied Cryptography* by A. Menezes, P. van Oorschot and S. Vanstone (CRC Press, 1996) are useful sources of information.

Evaluation:	2 Assignments	40%
	1 Research Project: (detailed outline 15%, writeup 30%, presentation 10%, class participation 5%)	60%

Outline: As this is the first time that this course has been offered, it is important to make it accessible to as many students as possible. This includes students in computer science and computer engineering. Thus, the course content will to some degree depend on the interests and background of the students enrolled. Nevertheless, broad areas will include:

- Fundamental concepts
  - one key cryptosystems
  - types of attack

  - one-way functions
  - one-way trap-door functions
  - two key cryptosystems

- Algorithms and hard problems
  - basic algorithms
  - primality testing
  - the discrete logarithm problem (DLP)

- Public-key cryptosystems
  - key exchange
  - the RSA scheme
  - the integer factoring problem
  - The Rabin-Williams scheme
  - the ElGamal scheme
  - the Digital Signature Algorithm (DSA)

- Probabilistic public-key cryptosystems
  - the quadratic residuosity problem
  - the Goldwasser-Micali scheme
  - the Blum-Goldwasser scheme

- Protocols
  - coin flipping by telephone
  - oblivious transfer
  - interactive proof schemes
  - zero knowledge proofs of identity