UNIVERSITY OF CALGARY

FACULTY OF SCIENCE

Mathematics and Statistics - MS 476
Ph: (403) 220-5203

COURSE INFORMATION SHEET

WINTER 2007

1. **Course:** **PMAT 629 / CPSC 601.09** -- Elliptic Curves & Cryptography
   Lecture/Time/Session: L01, TR 09:30-10:45, Winter 2007
   Instructor: Dr. Renate Scheidler, MS 364, 220-6628
   Office Hours: by appointment
   E-mail: rscheidl@math.ucalgary.ca
   Website: http://www.math.ucalgary.ca/~rscheidl/PMAT629

2. **Prerequisites:** PMAT 315 or equivalent, or consent of instructor
   PMAT 329 or PMAT/CPSC 669 or equivalent recommended

3. **Fee policy:** After the last day to drop/add courses, there will be no refund of tuition fees if a student withdraws from a course, courses or the session. **January 19, 2007** - Last day for changing registration in Winter Session half courses. No fee refunds after this date.

4. **Academic Accommodations**: It is the student's responsibility to request academic accommodations. A student with a documented disability who may require academic accommodation must register with the Disability Resource Centre to be eligible for formal academic accommodation. DRC registered students are required to discuss their needs with the instructor no later than fourteen (14) days after the start of this course.

5. The University policy on grading and related matters is described on pp. 43-45 of the 2006-2007 Calendar. In determining the overall grade in the course, the following weights will be used:

Assignments [3]	40%
Research Project	60% (Proposal 10%, Report 40%, Presentation 10%)

   The course **will not** have a Registrar's scheduled final examination.

   Special regulations affecting the final grade (e.g. requirement to pass the final examination or to pass the laboratory to pass the course): Each of the above components will be given a letter grade using the official University grading system. The final grade will be calculated using the grade point equivalents weighted by the percentages given above and then reconverted to a final letter grade using the official University grade point equivalents.

6. **Academic misconduct** (cheating, plagiarism, or any other form) is a very serious offence that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under the heading "Student Misconduct" (pages 53-56 for 2006-2007).

7. **Missed Components of Term Work**. The regulations of the Faculty of Science pertaining to this matter are outlined on page 198, of the 2006-2007 Calendar. It is the student's responsibility to familiarize himself/herself with these regulations.

8. **REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME ACTIVITY**. If you have a clash with an out-of-class-time activity, please inform your instructor at least one week in advance of the activity so that other arrangements may be made for you.

9. **Recommended Texts:**
   1. Guide to Elliptic Curve Cryptography
      Darrel R. Hankerson, Alfred J. Menezes and Scott Vanstone (*Springer*)
   2. Elliptic Curves: Number Theory and Cryptography
      Lawrence C. Washingon (*CRC Press*)