### UNIVERSITY OF CALGARY

## DEPARTMENT OF COMPUTER SCIENCE

### COURSE OUTLINE

COURSE: CPSC 629, Elliptic Curves and Cryptography (Cross-listed with PMAT 629)

LECTURE SECTIONS:

L01, MWF 11:00-11:50, Michael Jacobson, ICT 612, 210-9410, jacobs@ucalgary.ca, Office Hours: M 12:00-14:00

- 2. PREREQUISITES: Consent of the Department
- 3. GRADING: The University Policy on grading and related matters is described in sections F.1 and F.2 of the online University Calendar. In determining the overall grade in the course, the following weights will be used:

Assignments 40% Research Project 60%

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

Special Regulations affecting the Final Grade: Please see attached Grading Scheme.

- 4. MISSED COMPONENTS OF TERM WORK: The regulations of the Faculty of Science pertaining to this matter are found of the Faculty of Science area of the calendar in section 3.6: <a href="http://www.ucalgary.ca/pubs/calendar/current/sc-3-6.html">http://www.ucalgary.ca/pubs/calendar/current/sc-3-6.html</a>. It is the student's responsibility to familiarize themself with these regulations. See also <a href="http://www.ucalgary.ca/pubs/calendar/current/e-3.html">http://www.ucalgary.ca/pubs/calendar/current/e-3.html</a>.
- REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME-ACTIVITY. If you have a clash with this out-of-class-time-activity, please inform your instructor as soon as possible so that alternative arrangements may be made for you.
- 6. TEXTBOOK: None.
- EXAMINATION POLICY: Students are expected to provide proof of identity at any examination or test
  conducted in this course and to sign a class list if required. Section G in the University Calendar on
  Examinations: <a href="http://www.ucalgary.ca/pubs/calendar/current/g.html">http://www.ucalgary.ca/pubs/calendar/current/g.html</a>.
- 8. Optional course material, for which there may be a charge, may be made available during this course.
- Last Day to Drop a Class: January 20<sup>th</sup>, 2012
   Last Day to Add/Swap a Class: January 23<sup>rd</sup>, 2012
   Fee Payment Deadline: January 27<sup>th</sup>, 2012

#### 10. OTHER IMPORTANT INFORMATION FOR STUDENTS:

- a) 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 K. Student Misconduct <a href="http://www.ucalgary.ca/pubs/calendar/current/k.html">http://www.ucalgary.ca/pubs/calendar/current/k.html</a> to inform yourself of definitions, processes and penalties.
- b) ASSEMBLY POINTS: In case of emergency during class time. Be sure to familiarize yourself with the information at <a href="http://www.ucalgary.ca/emergencyplan/assemblypoints">http://www.ucalgary.ca/emergencyplan/assemblypoints</a>
- c) ACADEMIC ACCOMMODATION POLICY: Students with documented disabilities are referred to the following links: Calendar entry on students with disabilities: <a href="http://www.ucalgary.ca/pubs/calendar/current/b-1.html">http://www.ucalgary.ca/pubs/calendar/current/b-1.html</a>. Disability Resource Centre: <a href="http://www.ucalgary.ca/drc/">http://www.ucalgary.ca/drc/</a>
- d) SAFEWALK: Campus Security will escort an individual day or night, <a href="http://ucalgary.ca/security/safewalk">http://ucalgary.ca/security/safewalk</a>. Call 220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.
- e) FREEDOM OF INFORMATION AND PRIVACY: This course is conducted in accordance with the FOIPP Act. As one consequence, students must identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information see also <a href="http://www.ucalgary.ca/secretariat/privacy">http://www.ucalgary.ca/secretariat/privacy</a>.
- f) STUDENT UNION INFORMATION: VP Academic Phone: 220-3911, Email: <a href="mailto:suvpaca@ucalgary.ca">suvpaca@ucalgary.ca</a>. SU Faculty Rep. Phone: 220-3913. Email: <a href="mailto:sciencerep@su.ucalgary.ca">sciencerep@su.ucalgary.ca</a>. Website: <a href="http://www.su.ucalgary.ca/home/contact.html">http://www.su.ucalgary.ca/home/contact.html</a>. Student Ombudsman: <a href="http://www.su.ucalgary.ca/services/student-services/student-rights.html">http://www.su.ucalgary.ca/services/student-services/student-rights.html</a>.
- g) INTERNET and ELECTRONIC COMMUNICATION DEVICE Information: You can assume that in all your classes that you attend, your cell phone should be turned off. Also communication with other individuals via laptop computers, Blackberries or other devices connectable to the internet is not allowed in class time unless specifically permitted by the instructor. If you violate this policy you may be asked to leave the classroom. Repeat abuse may result in a charge of misconduct.

# UNIVERSITY OF CALGARY DEPARTMENT OF COMPUTER SCIENCE

CPSC/PMAT 629 Grading Scheme

Each of the graded components will be given a percentage grade. Your final percentage grade will be determined as a weighted average of each of the above components using the weights indicated on the course information sheet. This percentage will be converted to a letter grade using the following table:

95% to 100%:	A+
90% to 94%:	Α
85% to 89%:	A-
80% to 84%:	B+
75% to 79%:	В
70% to 74%:	B-
65% to 69%:	C+
60% to 64%:	C
55% to 59%:	C-
50% to 54%:	D+
45% to 49%:	D
0% to 44%	F