UNIVERSITY OF
CALGARY

DEPARTMENT OF COMPUTER SCIENCE
COURSE OUTLINE

1. **Course:** CPSC 669: Cryptography
(Crosslisted with PMAT 669)

Lecture Sections:

L01, MWF 9:00-9:50, MS 431, Michael Jacobson, ICT 612, 210-9410, jacobs@ucalgary.ca
Office Hours: MW 13:00-13:50

Course Website: http://pages.cpsc.ucalgary.ca/~jacobs/Courses/cpsc669/F14/index.html

Computer Science Department: ICT 602, 220-6015, cpsc@cpsc.ucalgary.ca

2. **Prerequisites:** Consent of the Department
(http://www.ucalgary.ca/pubs/calendar/current/computer-science.html#3620)

3. **Grading:** The University policy on grading and related matters is described 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 (3)	40%
Research Project	60%

This course **will not** have a Registrar's Scheduled Final Exam.

Special Regulations affecting the Final Grade: Grades for each of the above components will be awarded as percentages. Your final percentage grade will be determined as a weighted average of each of the above components using the weights indicated on the course outline. The final percentage grade will be converted to a letter grade using the attached table.

4. **Missed Components of Term Work:** The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar in Section 3.6. It is the student's responsibility to familiarize himself/herself with these regulations. See also Section E.6 of the University Calendar

5. **Scheduled out-of-class activities:** None.

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. **Course Materials:** None.

Online Course Components: None.

7. **Examination Policy**: No examination in this course.

8. **Approved Mandatory and Optional Course Supplemental Fees**: None.

9. **Writing across the curriculum statement:** In this course, the quality of the student's writing in course components will be a factor in the evaluation of the course components. See also Section E.2 of the University Calendar.

10. **Human studies statement:** See Section E.5 of the University Calendar.

11. **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 Section K. Student Misconduct 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 on assembly points.

(c) **Academic Accommodation Policy:** Students with documentable disabilities are referred to the following: Calendar entry on students with disabilities and Student Accessibility Services.

(d) **Safewalk:** Campus Security will escort individuals day or night (http://www.ucalgary.ca/security/safewalk/). 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 Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence, students should 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: http://www.ucalgary.ca/secretariat/privacy

(f) **Student Union Information:** VP Academic, 220-3911, suvpaca@ucalgary.ca
SU Faculty Rep, 220-3913, sciencerep@su.ucalgary.ca

(g) **Internet and Electronic Device Information:** You can assume that in all classes that you attend, your cell phone should be turned off unless instructed otherwise. 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. Repeated abuse may result in a charge of misconduct.

(h) At the University of Calgary, feedback provided by students through the Universal Student Ratings of Instruction (USRI) survey provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses (www.ucalgary.ca/usri). Your responses make a difference - please participate in USRI Surveys.

Department Approval Cory Williamson Date Sept 4/14

CPSC 669 Syllabus

CPSC 669 Course Description:

An overview of basic techniques in modern cryptography, with emphasis on fit-for-application primitives and protocols. Topics to include symmetric and public-key cryptosystems; digital signatures; elliptic curve crypgoraphy; key management; attack models and well-defined notions of security.

Tentative Topics Covered:

Topic 1: Symmetric cryptography

- introduction to cryptography and cryptanalysis
- substitution ciphers (redundancy, entropy, unicity distance, perfect security and the one-time pad)
- block ciphers (3DES, AES, modes of operation)
- data integrity (hash functions and message authentication codes

Topic 2: Public-key cryptography

- extended Euclidean algorithm, binary exponentiation, Euler phi-function, primitive roots
- one-way functions, Diffie-Hellman key exchange
- one-way trapdoor functions, RSA
- quadratic residuosity, Jacobi symbol, square roots modulo a prime
- Provable PKC (randomized encryption, El Gamal, semantic security, Goldwasser-Micali, indistinguishability, RSA-OAEP)
- Digital signatures (El Gamal, DSA)
- elliptic curve cryprography (elliptic curves, elliptic curve key agreement)

Topic 3: Cryptography in practice

- Key management (pseudorandom number generation, public-key infrastructures)
- Email security (PGP)
- secure shell (ssh)

CPSC/PMAT 669 Percentage to Letter Grade Conversion Table

A+	95-100
A	90-94
A-	85-89
B+	80-84
B	75-79
B-	70-74
C+	65-69
C	60-64
C-	55-59
D+	50-54
D	40-49
F	0-39