UNIVERSITY OF CALGARY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS & STATISTICS
COURSE OUTLINE

1. **Course:** PMAT 429, Cryptography-Design and Analysis of Cryptosystems -- Winter 2018

   Lecture 01: (MWF, 15:00-15:50 in MS319)

Instructor Name	Email	Phone	Office	Hours
Mark Bauer	bauerm@ucalgary.ca	4032108456	MS 558	TBA

   Course Site:

   D2L: PMAT 429 L01-(Winter 2018)-Cryptography-Design and Analysis of Cryptosystems

   Department of Mathematics & Statistics: MS 476, 403 220-5210,

   Students must use their U of C account for all course correspondence.

2. **Prerequisites:**

   See section 3.5.C in the Faculty of Science section of the online Calendar.

   Pure Mathematics 315 or 317; and one of Pure Mathematics 329, 418, Computer Science 418.

3. **Grading:**

   The University policy on grading and related matters is described in F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:

Component(s)	Weighting %
Homework (5)	30%
Midterm test	30% (tentatively March 2)
Presentation	10%
Term Project	30%

   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 converted to a final letter grade using the official university grade point equivalents.

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.3 of the University Calendar

5. **Scheduled out-of-class activities:**

   There are no out-of-class activities scheduled for this course.

   REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME-ACTIVITY. If you have a conflict with the out-of-class-time-activity, please contact your course coordinator/instructor no later than **14 days prior** to the date of the out-of-class activity so that alternative arrangements may be made.

6. **Course Materials:**

Required Textbook. An Introduction to Mathematical Cryptography, Hoffstein, Pipher, and Silverman. Springer. Available for free through SpringerLink

7. **Examination Policy:**

   No aids are allowed on tests or examinations

   Students should also read the Calendar, Section G, on Examinations.

8. **Approved Mandatory and Optional Course Supplemental Fees:**

   There are no mandatory or optional course supplemental fees for this course

9. **Writing across the Curriculum Statement:**

   For all components of the course, in any written work, the quality of the student's writing (language, spelling, grammar, presentation etc.) can be a factor in the evaluation of those reports. See also Section E.2 of the University Calendar.

10. **Human studies statement:**

    Students will not participate as subjects or researchers in human studies.

11. **Reappraisal of Grades:**

    A student wishing a reappraisal, should first attempt to review the graded work with the Course coordinator/instructor or department offering the course. Students with sufficient academic grounds may request a reappraisal. Non-academic grounds are not relevant for grade reappraisals. Students should be aware that the grade being reappraised may be raised, lowered or remain the same. See Section I.3 of the University Calendar.

    1. **Term Work:** The student should present their rationale as effectively and as fully as possible to the Course coordinator/instructor within **15 days** of either being notified about the mark, or of the item's return to the class. If the student is not satisfied with the outcome, the student shall immediately submit the Reappraisal of Graded Term work form to the department in which the course is offered. The department will arrange for a re-assessment of the work if, and only if, the student has sufficient academic grounds. See sections I.1 and I.2 of the University Calendar
    2. **Final Exam:**The student shall submit the request to Enrolment Services. See Section I.3 of the University Calendar.

12. **OTHER IMPORTANT INFORMATION FOR STUDENTS:**

    a. **Misconduct:** 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. Examples of academic misconduct may include: submitting or presenting work as if it were the student's own work when it is not; submitting or presenting work in one course which has also been submitted in another course without the instructor's permission; collaborating in whole or in part without prior agreement of the instructor; borrowing experimental values from others without the instructor's approval; falsification/ fabrication of experimental values in a report. **These are only examples**.

    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 needing an accommodation because of a disability or medical condition should contact Student Accessibility Services in accordance with the procedure for accommodations for students with disabilities available at procedure-for-accomodations-for-students-with-disabilities_0.pdf.

       Students needing an accommodation in relation to their coursework or to fulfill requirements for a graduate degree, based on a protected ground other than disability, should communicate this need, preferably in writing, to the Associate Head of the Department of Mathematics & Statistics, Jim Stallard by email jbstall@ucalgary.ca or phone 403-220-3953. Religious accommodation requests relating to class, test or exam scheduling or absences must be submitted no later than **14 days** prior to the date in question: http://www.ucalgary.ca/pubs/calendar/current/e-4.html

    d. **Safewalk:** Campus Security will escort individuals day or night (www.ucalgary.ca/security/safewalk/) . Call 403-220-5333 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). 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 www.ucalgary.ca/legalservices/foip.

f. **Student Union Information:** VP Academic, Phone: 403-220-3911 Email: suvpaca@ucalgary.ca. SU Faculty Rep., Phone: 403-220-3913 Email: sciencerep@su.ucalgary.ca. Student Ombudsman, Email: suvpaca@ucalgary.ca.

g. **Internet and Electronic Device Information:** Unless instructed otherwise, cell phones should be turned off during class. All communication with other individuals via laptop, tablet, smart phone or other device is prohibited during class unless specifically permitted by the instructor. Students that violate this policy may be asked to leave the classroom. Repeated violations may result in a charge of misconduct.

h. **Surveys:** At the University of Calgary, feedback through the Universal Student Ratings of Instruction (USRI) survey and the Faculty of Science Teaching Feedback form provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses. Your responses make a difference - please participate in these surveys.

i. **SU Wellness Center:** The Students Union Wellness Centre provides health and wellness support for students including information and counselling on physical health, mental health and nutrition. For more information, see www.ucalgary.ca/wellnesscentre or call 403-210-9355.

Department Approval: Electronically Approved **Date:** 2017-12-22 11:15

Course Outcomes

1. analyze the e
2. fficiency of basic algorithms used in cryptography, both in terms of run-time and storage.
3. apply number theoretic algorithms and concepts to cryptanalyze public- key cryptographic primitives.
4. demonstrate competence with algorithms for integer factorization, solving discrete logarithm problems, primality testing and elliptic curves.
5. restate the main cryptographic protocols that are covered in the course and their different functions
6. use mathematical reasoning to rigorously prove security, efficiency, and correctness of various cryptographic primitives
7. apply complexity results for number theoretic algorithms to determine appropriate parameter selection, security assessment, and effi
8. ciency of public-key cryptographic primitives.