FACULTY OF SCIENCE – MATHEMATICS & STATISTICS - MS 476
Ph: (403) 220-5203; E-mail: undergrad@math.ucalgary.ca

UNIVERSITY OF
CALGARY

COURSE OUTLINE

WINTER 2013

1. **PMAT 429 Cryptography – Design and Analysis of Cryptosystems**

Lec	Day	Time	Instructor	Office	Phone	Email	Office Hours
L01	MWF	10:00-10:50	Renate Scheidler	MS 458	220-6628	rscheidl@ucalgary.ca	W 14:00 – 15:00

2. **Prerequisites**: Pure Mathematics 315 or 317; and one of Pure Mathematics 329, 418, Computer Science 418 (see Section 3.5C of Faculty of Science www.ucalgary.ca/pubs/calendar/current/sc-3-5.html and Course Descriptions: www.ucalgary.ca/pubs/calendar/current/course-desc-main.html)

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	[3]	30 %	
Presentation		10 %	
Report		10 %	
Midterm Test		15 %	(Tentatively March 6th in class)
Final Exam		35 %	(To be scheduled by the Registrar's Office)

The various components above will be assigned a percentage score and will be combined with the indicated weights to produce an overall percentage in the course. The conversion table between course percentage and letter grade will be provided at least one week before the withdrawal deadline.

A passing grade in the Final Examination is essential for an overall grade of C- or better.

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: www.ucalgary.ca/pubs/calendar/current/sc-3-6.html**.** It is the student's responsibility to be familiar with these regulations. See also www.ucalgary.ca/pubs/calendar/current/e-3.html.

5. **There will be no out of class time activity.**

REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME ACTIVITY. If you have a conflict with any 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.

6. **Textbooks** (*recommended*):
   Johannes Buchmann, *Introduction to Cryptography*, 2nd edition, Springer, 2004
   Lawrence C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd edition, CRC Press, 2008

7. **Examination Policy**: Students are NOT permitted any aids during the midterm or final exam. Students should also read the Calendar, Section G, on Examinations: www.ucalgary.ca/pubs/calendar/current/g.html

8. **Writing across the curriculum: i**n this course, the quality of the student's writing in assignments and reports will be a factor in the evaluation of those reports. See also http://www.ucalgary.ca/pubs/calendar/current/e-2.html.

9. **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 (http://www.ucalgary.ca/pubs/calendar/current/k.html) 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 http://www.ucalgary.ca/emergencyplan/assemblypoints.

(c) ACADEMIC ACCOMMODATION POLICY. Students with documentable disabilities are referred to the following links:
Calendar entry on students with disabilities: http://www.ucalgary.ca/pubs/calendar/current/b-1.html
Disability Resource Centre: http://www.ucalgary.ca/drc/

(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 **Phone**: 220-3911 **Email**: suvpaca@ucagary.ca.
SU Faculty Rep. **Phone:** 220-3913 **Email:** sciencerep@su.ucalgary.ca **Website** http://www.su.ucalgary.ca/
Student Ombudsman: http://www.ucalgary.ca/provost/students/ombuds

(g) INTERNET and ELECTRONIC COMMUNICATION DEVICE Information. You can assume that in all 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. Repeated abuse may result in a charge of misconduct.

FACULTY OF SCIENCE - MATHEMATICS & STATISTICS – MS 476
Ph: (403) 220–5203; E–mail: undergrad@math.ucalgary.ca

UNIVERSITY OF CALGARY

COURSE OUTLINE

ADDENDUM - GRADING POLICY

WINTER 2013

1. **PMAT 429 Cryptography – Design and Analysis of Cryptosystems**

Lec	**Day**	**Time**	**Instructor**	**Office**	**Phone**	**Email**	**Office Hours**
L01	MWF	10:00-10:50	Renate Scheidler	MS 458	220-6628	rscheidl@ucalgary.ca	W 14:00 – 15:00

2. **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	[3]	30 %	
Presentation		10 %	
Report		10 %	
Midterm Test		15 %	(Tentatively March 6th in class)
Final Exam		35 %	(To be scheduled by the Registrar's Office)

Each piece of work submitted by the student will be assigned a percentage score. The average percentage score for each item of a term component will be combined with its course component weighting listed above to form a weighted average which is to be the final score in the course. This final score, a percentage out of 100, will then be converted to a letter grade using the following conversion table:

≥ 90	A+, A, A-
≥ 75	B+, B, B-
≥ 60	C+, C, C-
≥ 50	D, D-
< 50	F