UNIVERSITY OF CALGARY
FACULTY OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
COURSE OUTLINE

1. **Course:** CPSC 418: Introduction to Cryptography
   Lecture Sections:
   L01, MWF 15:00-15:50, SA 104, Renate Scheidler, MS 436, 220-6628, rscheidl@ucalgary.ca
   Office Hours: M 16:00-17:00 W 10:30-11:30

   Course Website: people.ucalgary.ca/~rscheidl/418

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

2. **Prerequisites:** Either CPSC 331 or CPSC 319 and 105, and one of MATH 271, 273, or PMAT 315 (http://www.ucalgary.ca/pubs/calendar/current/computer-science.html#3620)

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 (4)	40%	
(Due: Oct 7th, Oct 28th, Nov 18th, Dec 9th)		
Midterms (2)		30%
(Midterm #1: In-Class Friday October 21st, 2016)		
(Midterm #2: In-Class Friday November 25th, 2016)		
Final Exam	30%	

   This course **will** have a Registrar's Scheduled Final Exam.

   Special Regulations affecting Final grade: None.

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. Section 3.6. It is the student's responsibility to familiarize theirself with these regulations. See also Section E.6 of the University calendar.

5. **Scheduled Out-of-Class Activities:** REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME ACTIVITY. If you have a clash with this out-of-class activity, please inform your instructor as soon as possible so that alternative assignments can be arranged.

6. **Course Materials:**
   Cryptography Theory and Practice 3rd Edition, D. Stinson, *Chapman & Hall/CRC* 2006 (Recommended)

   Online Course Components:
   Lecture slides, assignments and handouts will be available on the course webpage.

7. **Examination Policy:** Closed book. No aids of any kind are permitted. Students should also read the Calendar, Section G, on examinations.

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 the weighted components of the course will be a factor in the evaluation of these components. See also Section E.2 of the University Calendar.

10. **Human Studies Statement:** Students will be expected to participate as subjects or participants in projects. See also Section E.5 of the University Calendar.

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

a) **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offense 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 which can be found in each classroom and building.

c) **Student Accommodations:** 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 http://www.ucalgary.ca/policies/files/policies/procedure-for-accommodations-for-students-with-disabilities_0.pdf. Students needing an Accommodation in relation to their coursework or to fulfil 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 Computer Science.

d) **Safewalk:** Campus Security will escort individuals day or night (http://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). 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 (403) 220-3911 suvpaca@ucalgary.ca SU Faculty Rep (403) 220-3913 science1@su.ucalgary.ca, science2@su.ucalgary.ca and science3@su.ucalgary.ca, Student Ombuds Office: (403) 220-6420 ombuds@ucalgary.ca, http://ucalgary.ca/provost/students/ombuds

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. All communications with other individuals via laptop computers, cell phones or other devices connectable to the internet in not allowed during 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) **U.S.R.I.:** 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_____Date_____

Associate Dean's Approval for
out of regular class-time activity: _____Date:_____

Associate Dean's Approval for
Alternate final examination
arrangements:_____Date:_____

A signed copy of this document is kept on file in the Computer Science main Office ICT 602

CPSC 418 Percentage to Letter Grade Conversion Table

A+	95-100
A	90-95
A-	86-90
B+	82-86
B	78-82
B-	74-78
C+	70-74
C	66-70
C-	62-66
D+	58-62
D	50-58
F	0-50

CPSC 418 Syllabus

Week	Tentative Topics Covered
1	Introduction and motivation, attack models, symmetric cryptosystems, notions of security
2	Classical ciphers, probability theory, perfect secrecy
3	More on perfect secrecy, one-time pad, entropy
4	Product ciphers, Data Encryption Standard
5	Advanced Encryption Standard
6	Cryptanalysis of block ciphers, stream ciphers, modes of operation of block ciphers
7	Hash functions and message authentication codes
8	One-way functions, number theory, the Diffie-Hellman protocol
9	Public key cryptosystems, more number theory, RSA
10	Efficiency and security of RSA, probabilistic encryption and ElGamal PKC, provable security under passive attacks
11	Quadratic residuocity, Goldwasser-Micali system, active attacks on RSA, provable security under active attacks, RSA-OAEP
12	Digital signatures, signatures from public key cryptosystems, security of signatures, El Gamal signature scheme, Digital Signature Standard
13	Cryptography in practice: key management and distribution, authentication, cryptographically secure pseudorandom bit generators, secure e-mail via PGP, access control via SSH

Learning Outcomes:

The main objective of this course is to provide students with a thorough understanding of the fundamentals of and current best practices in cryptography. Students will have a solid understanding, including practical experience, of the basic cryptographic primitives and their proper usage.Illustrative real world examples of cryptographic systems are used to demonstrate how cryptographic primitives can be combined to provide robust security assurances. In particular, a student who successfully completes this course will be able to:

1. describe the different services that cryptography provides and give examples of cryptographic mechanisms that provide a given service.
2. verify that a cryptographic mechanism works properly, eg. that encryption followed by decryption is successful.
3. describe the different attack models covered in the course and how they relate to each other.
4. demonstrate competence with mathematical foundations of modern cryptographic primitives.
5. apply mathematics to assess the security of cryptographic primitives.
6. restate the main cryptographic protocols that are covered in the course and their differentfunctions

In addition, students taking CPSC 418 will be able to

7. write software that provides cryptographic services and integrate existing cryptographic software libraries and packages in this software.

In addition, students taking PMAT 418 will be able to

7. use mathematical reasoning to rigorously prove security properties of various cryptographic primitives.