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

1. **Course:** CPSC 530: Information Theory and Security
CPSC 630: Information Theory and Security
Lecture Sections:
L01, TR 15:30-16:45, MS 527, Rei Safavi-Naeini, ICT 636, 210-5492, rei@ucalgary.ca
Office Hours: TR 13:00-14:00

Course Website: D2L

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

2. **Prerequisites:** CPSC 530: CPSC 219, 233 or 235, Math 271 or 273 or PMAT 315, and one of STAT 205, 211, 213, 321 or MATH 321
CPSC 630: 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 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:

CPSC 530		CPSC 630	
Assignments	45%	Assignments	30%
Midterm Exam	25%	Midterm Exam	25%
	(In-Class Thursday October 20th, 2016)		
Project	30%	Project	45%

This course **will not** 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 (Discrete Mathematics and its Applications) 3rd Edition, Douglas Stinson, *Chapman and Hall/CRC* (Reference)
Introduction to Modern Cryptography 2nd Edition, Jonathan Katz & Yehuda Lindell
Elements of Information Theory 2nd Edition, Thomas M. Cover & Joy A. Thomas, *Wiley* (Reference)

Online Course Components:
Lecture slides will be online or on D2L.

7. **Examination Policy:** Open book. 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 530/630 Percentage to Letter Grade Conversion Table

A+	90-100
A	85-89
A-	80-84
B+	77-79
B	73-76
B-	70-72
C+	67-69
C	63-66
C-	60-62
D+	55-59
D	50-54
F	0-49

CPSC 530/630 Syllabus

Tentative Topics Covered

- Measures of Information
- Correlation, similarity and distance
- Perfect Secrecy
- Message Authentication
- Secret sharing and distributed system security
- Randomness and random number generation
- Secure and reliable message transmission

Learning Outcomes:

By the end of the course: students will:

- state measures of information, and quantify similarity and correlation of random variables
- describe leakage of information and design encryption systems with perfect and near perfect secrecy
- model message corruption in communication due to noise and active tampering, and design protection systems guaranteed performance
- model security and reliability of distributed systems and design and evaluate coding systems for providing protection