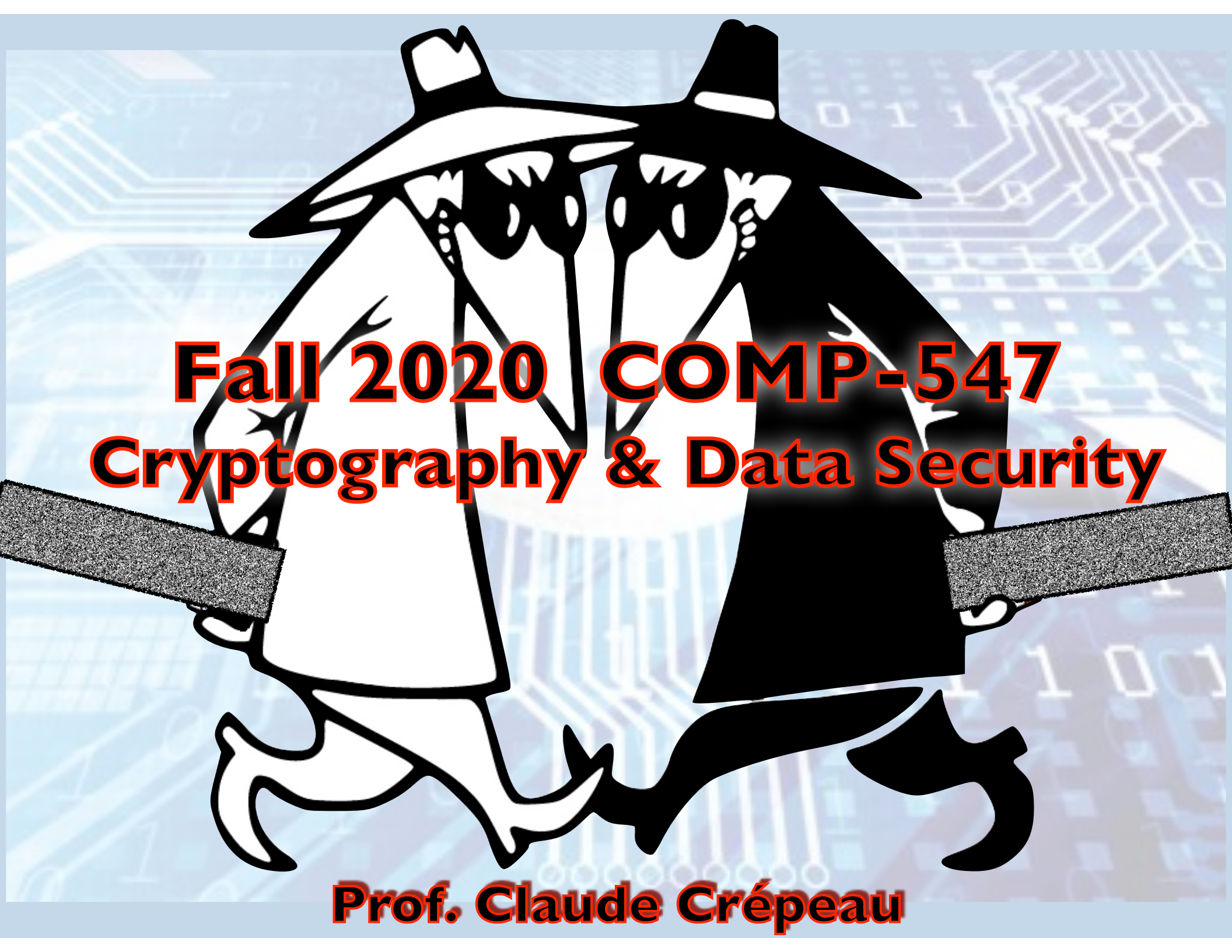

Fall 2020 COMP-547
Cryptography & Data Security
Prof. Claude Crépeau

ME

- **Prof. Claude Crépeau**
- **McConnell-110N**
- **(514) 398-4716**
- **Office Hours: Wednesdays 14:00-17:00**

- **For all class matters please use:**

  cs547@cs.mcgill.ca

  crepeau@cs.mcgill.ca

TA(s)

- Pouriya Alikhani
- McConnell 107
- Office Hours:
  Mondays 8:30-10:00

- Pouriya |Alikhani
- McConn|ell 107
- Office H|ours:
  Monday|s 8:30-10:00

- For all class matters please use:

cs547@cs.mcgill.ca

pouriya.alikhani@mail.mcgill.ca

COMP-547 Fall 2020 — Weekly Schedule

Pouriya MC-107 office hours	**Tue** 08:30	**Wed** 08:30	**Thu** 08:30	**Fri** 08:30
	Tue 09:00	**Wed** 09:00	**Thu** 09:00	**Fri** 09:00
	Tue 09:30	**Wed** 09:30	**Thu** 09:30	**Fri** 09:30
Mon 10:00	**Tue** 10:00	**Wed** 10:00	**Thu** 10:00	**Fri** 10:00
Mon 10:30	**Tue** 10:30	**Wed** 10:30	**Thu** 10:30	**Fri** 10:30
Mon 11:00	**Tue** 11:00	**Wed** 11:00	**Thu** 11:00	**Fri** 11:00
Mon 11:30	**Tue** 11:30	**Wed** 11:30	**Thu** 11:30	**Fri** 11:30
Mon 12:00	**Tue** 12:00	**Wed** 12:00	**Thu** 12:00	**Fri** 12:00
Mon 12:30	**Tue** 12:30	**Wed** 12:30	**Thu** 12:30	**Fri** 12:30
Mon 13:00	**Tue** 13:00	**Wed** 13:00	**Thu** 13:00	**Fri** 13:00
Mon 13:30	**Tue** 13:30	**Wed** 13:30	**Thu** 13:30	**Fri** 13:30
Mon 14:00	**Tue** 14:00	Claude MC-110N office hours	**Thu** 14:00	**Fri** 14:00
Mon 14:30	**Tue** 14:30		**Thu** 14:30	**Fri** 14:30
Mon 15:00	**Tue** 15:00		**Thu** 15:00	**Fri** 15:00
Mon 15:30	**Tue** 15:30		**Thu** 15:30	**Fri** 15:30
Mon 16:00	Claude online lecture		Claude online lecture	**Fri** 16:00
Mon 16:30				**Fri** 16:30
Mon 17:00		**Wed** 17:00		**Fri** 17:00

MC = MCENG = McConnell

COMMUNICATIONS

www:

via myCourses

email:

cs547@cs.mcgill.ca

FaceBook:

COMP 547 @ McGill

COMP-547
Cryptography & Data Security

Description:(4 credits; 3 hours) This course presents an in-depth study of modern cryptography and data security. We investigate four important subjects of cryptography:

- **key distribution,**
- **data encryption,**
- **data authentication,**
- **user identification.**

The basic information theoretic and computational security of classical and modern cryptographic systems are analyzed. The course is self-contained and all necessary math background will be covered.

COMP-547: textbook

Student Photos by CRN | McGill University School o | Comp610: Information Sti | Course Description -- Info | McGill School Of Compute | Honours Algorithm De

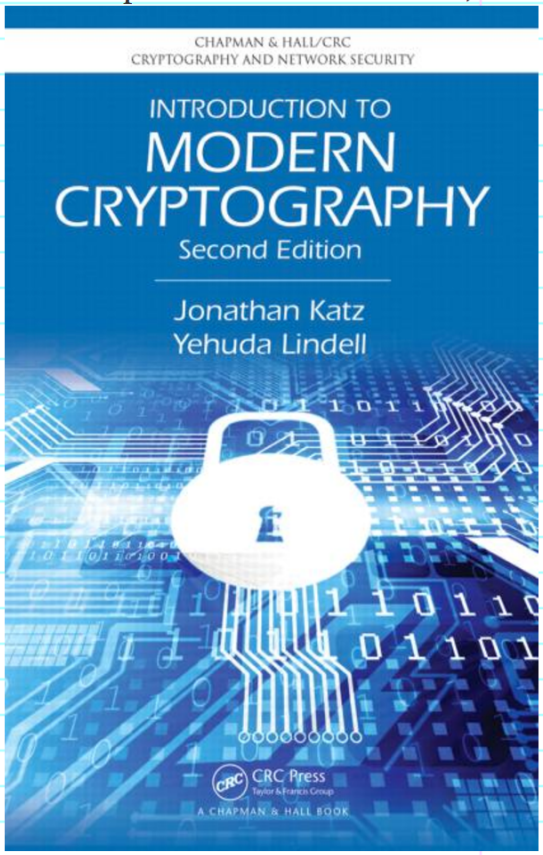
crepeau/COMP547/

ions | Divertissements | Spiritualité | Outils ou Référence | Apple | Mac help | Importés depuis Safari

Mandatory textbook:

Introduction to Modern Cryptography 2nd Edition , by Jonathan Katz and Yehuda Lindell.

Publisher: Chapman and Hall/CRC Press, Nov 2014.



Errata

COMP-547 : EVALUATION

Your final grade will be calculated as

- 60% for 4 assignments (15% each)
- 40% for the final exam
- The exam is open book — open documentation .

"In the event of extraordinary circumstances beyond the University's control, the evaluation scheme in a Course is subject to change, provided that there be timely communications to the students regarding the change."

COMP-547 : Collaborations

- We greatly encourage you to discuss the assignment problems with each other.
- However, these discussions should not go so far that you are sharing code or giving away the answer.
- A rule of thumb is that your discussions should be considered public in the sense that anything you share with a friend should be sharable with any student in the class.
- We ask you to indicate on your assignments the names of the persons with whom you collaborated or discussed your assignments (including the TA's and instructor).

COMP-547 : Grades

Policy on re-grading

- If you wish us to re-grade a question on an exam (or assignment), we will do so. However, to avoid grade ratcheting, we reserve us the right to re-grade other questions on as well.

Policy on final grades

- We will use the same rules and formula for calculating the final grade for everyone. We understand that your performances may be influenced by many factors, possibly out of your control. However, that is the only way we can be fair. The only exceptions will be medical exceptions. In that case, I will require a medical note, which has to be also reported to McGill, and to be informed as early as possible. Failure to comply to these rules, may results in the impossibility to invoke a medical exception.

COMP-547 : Assignments

Policy on Assignments

- Due date/time, location/mode for returning your solutions, and accepted formats will be announced in class and indicated on the course web page.
- Failure to return your assignment in time will result in penalties or even absence of grading. Late submission of 24h or less may receive a penalty of 20%. In all other cases, your assignment shall be refused and not graded.

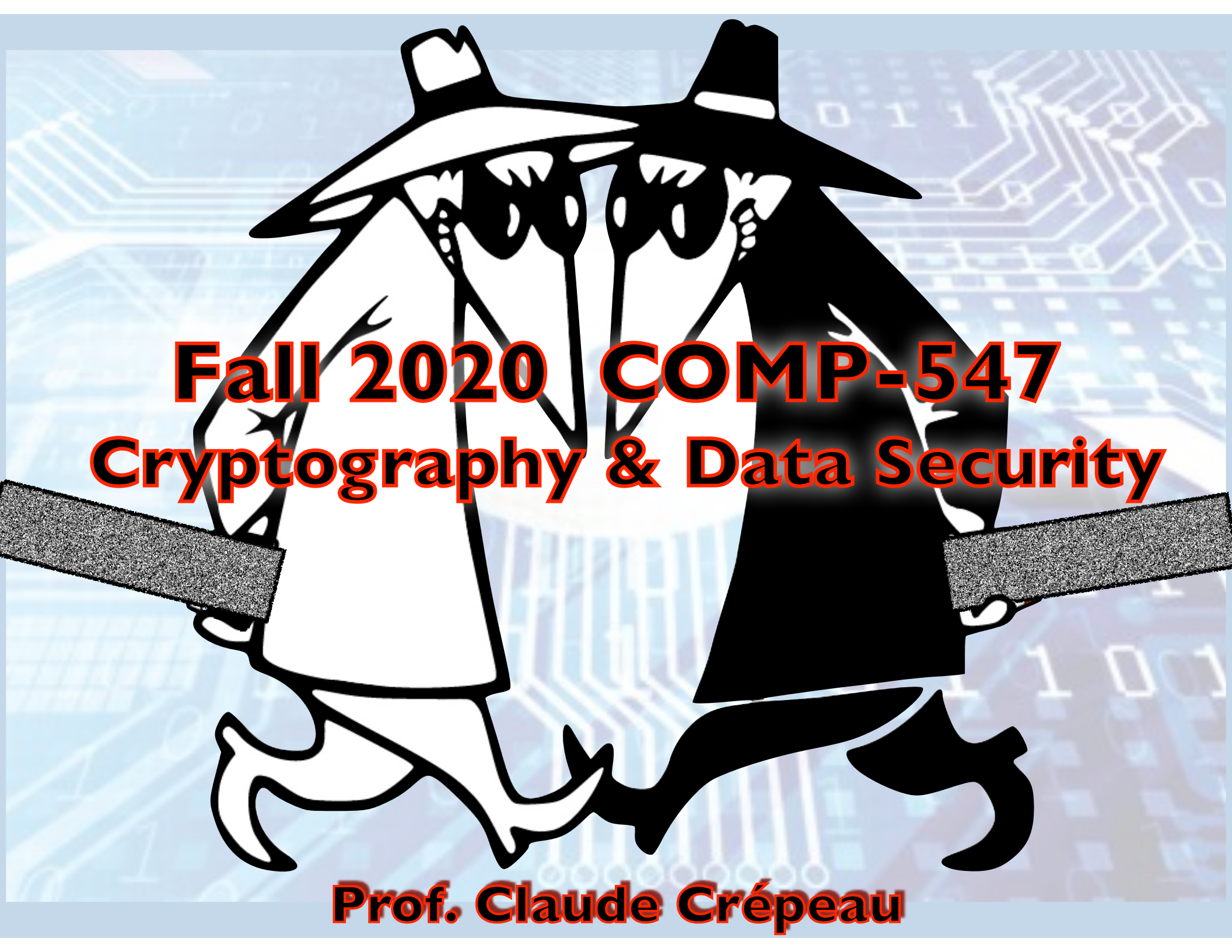
COMP-547 : Assignments

- Importantly, solutions that do not follow the requested format will receive a penalty. By default, we only accept PDF or TEXT files. Images must be embedded in a PDF. Do not compress your files. All files must open on LINUX SOCS workstations.
- The quality of the presentation of your solutions is very important. Unreadable material, cryptic notations, or bad organization will results in penalties, and potentially even an absence of grading. If you scan your hand-written solutions, it is your responsibility to ensure that you submit a high-quality image (i.e. excellent luminosity, contrast, focus and resolution). The clarity of your explanations will also be an integral part of your grade.

COMP-547 : @McGill

McGill Policies

- In accordance with McGill University's Charter of Students' Rights, students in this course have the right to submit in French as well as in English any written work that is to be graded.
- McGill University values academic integrity. Therefore, all students must understand the meaning and consequences of cheating, plagiarism and other academic offenses under the Code of Student Conduct and Disciplinary Procedures.


Fall 2020 COMP-547
Cryptography & Data Security
Prof. Claude Crépeau