Semester Plan and Timetable
COSC362: Data and Network Security

Spring 2021

The following plan and timetable **may still be adjusted** during the semester.

1 Important dates

- Course start date: 19 July 2021.
- Course end date: 22 October 2021.
- Break: 30 August – 10 September.

- Quiz deadline: (almost) every Friday at 23:59. Please check below.
- Assignment deadline: 17 September 2021.
- Final examination date: *to be announced*.

2 Assessment summary

1. **Labs** (10%):
   - You are highly encouraged to attend all labs during the semester.
   - Labs are done individually but you are encouraged to discuss and share with your peers (you are allowed to see each other during labs).
   - Attending one lab each week over the semester automatically gives you **full mark**:
     - The tutor will assess your attendance.
   - If you cannot attend one lab session, then a report (along with a justification of student absence) will be required and assessed:
     - The report needs to be submitted by one week after the missed session.
     - *Example:* if you miss Tuesday lab on Week X then you are asked to submit a report by Tuesday of Week X+1.
     - The report needs to be sent to **both** the lecturer and the tutor.

2. **Weekly quizzes** (20%):

   - 9 quizzes in total.
   - Each quiz contains 10 questions. Each question contains 4 choices such that **only one choice is correct**.
   - They can be found and done on LEARN.
   - 2 attempts per quiz, such that the highest grade is taken into account.
   - A quiz is given on Friday of Week X, and should be done before Friday of Week X+1 (except for the one released just before the break):

Quiz	Released on	Due on	Answers available from
1	Friday 06/08	Friday 13/08	Monday 16/08
2	Friday 13/08	Friday 20/08	Monday 23/08
3	Friday 20/08	Friday 27/08	Monday 30/08
4	Friday 27/08	Friday 17/09	Monday 20/09
5	Friday 17/09	Friday 24/09	Monday 27/09
6	Friday 24/09	Friday 01/10	Monday 04/10
7	Friday 01/10	Friday 08/10	Monday 11/10
8	Friday 08/10	Friday 15/10	Monday 18/10
9	Friday 15/10	Friday 22/10	Monday 25/10

3. **Assignment** (20%):

   - Small exercises on what has been covered so far.
   - The assignment will be released on LEARN on 20 August 2021.
   - Deadline: **17 September 2021**.
   - Your report should be uploaded to LEARN.

4. **Final examination** (50%):

   - A mix of multiple-choice questions (as for online quizzes) and small exercises (as in the assignment). More precisely:
     - **25 multiple-choice questions** s.t. one question has 4 possible choices and **only one is correct** (as for the LEARN quiz).
     - (around) **5 open questions** (such as the ones in the assignement), such that if additional information is needed to solve the problem then it will be provided.
   - Syllabus mainly defined by the lecture slides and some labs:
     - **All** contents from **all** lecture slides are part of the syllabus. You are exepcted to study definitions, mechanisms, processes, etc. of maths tools, crypto algorithms, crypto systems, crypto applications, etc. However:

        * I do not ask you to remember the code of each standard (e.g. RFC 1234)!!
        * I do not ask you to remember the chronology/history of all the algorithms/systems we have seen (e.g. the attack X against Y was launched in 2006).
        * In summary, all the small details are **not** part of the syllabus.
    - **Maths-related exercises** such as the ones covered in **Labs 2 and 6** can be found in the exam.
    - **On-paper exercises** such as the ones covered in **Labs 7, 9 and 11** can be found in the exam.
    - Practical labs (CrypTool – 3, 4, 5; PKI – 8; TLS – 10) are **not** part of the syllabus.
    - Stallings' textbooks are **not** part of the syllabus:
        * More precisely, exam questions will not contain items that you can find in the books but not in the lecture slides.
- Date: *to be announced*
- Time: *to be announced* (3 hours)
- Permitted materials:
    - Calculator with a UC sticker approved
    - Writing items (pencils, rubbers)
    - One A4 hand-written sheet of paper ("cheat sheet") such that it can be double side but it has to be strictly hand-written by the student, not printed and not a reduced version of someone's notes

2.1 Miscellaneous

Additional material to be found on LEARN:

- Lab sheets with both questions and answers
- Quiz sheets with both questions and answers
- Forum section:
    - There is an anonymity feature, so use it!
    - I encourage you to post your questions there (rather than sending me emails).
    - I hope that questions will be asnwered among peers (rather than relying on me).

Textbooks:

- *Cryptography and network security : principles and practice*, William Stallings, 5th edition:
    - One copy at UC library.
- *Computer security : principles and practice*, William Stallings and Lawrie Brown, 3rd edition:
    - 4 copies at UC library.

Course lecturer: Clémentine Gritti

- clementine.gritti@canterbury.ac.nz
- Office: Jack Erskine 304
- Office hours: no specific ones, just send an email to check.

Teaching assistant: Ryan Beaumont

- rbe72@uclive.ac.nz