

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: 2 November 2021 from 2:30pm to 5:30pm.

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%):

- 8 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~~ Tuesday of Week X, and should be done before ~~Friday~~ Tuesday of Week X+1 (except for the one released just before the break):

Quiz	Relates to	Released on	Due on	Answers available from
1	Lectures 3, 5 and 6	Friday 06/08	Friday 13/08	Monday 16/08
2	Lectures 7 and 8	Friday 13/08	Friday 20/08 27/08	Monday 23/08 30/08
3	Lectures 9 and 10	Tuesday 24/08	Tuesday 14/09	Wednesday 15/09
4	Lectures 11 and 12	Tuesday 14/09	Tuesday 21/09	Wednesday 22/09
5	Lectures 13 and 14	Tuesday 21/09	Tuesday 28/09	Wednesday 29/09
6	Lectures 15 and 16	Tuesday 28/09	Tuesday 05/10	Wednesday 06/10
7	Lectures 17 and 18	Tuesday 12/10	Tuesday 19/10	Wednesday 20/10
8	Lectures 19 and 20	Tuesday 19/10	Tuesday 26/10	Wednesday 27/10

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:
 - **30 multiple-choice questions** s.t. one question has 4 possible choices and **only one is correct** (as for the LEARN quiz):
 - * You will need to tick the box of the answer that you think it is the correct one.
 - **12 open questions** grouped into 6 exercises (such as the ones in the assignment), such that if additional information is needed to solve the problem then it will be provided:
 - * You will need to insert your answer directly in the box. The number of lines is limited to 15.
- Syllabus mainly defined by the lecture slides and some labs:

- **All** contents from **all** lecture slides are part of the syllabus. You are expected 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 5** can be found in the exam.
- **On-paper exercises** such as the ones covered in **Labs 6, 9 and 11** can be found in the exam.
- Practical labs (CrypTool – 3, 4, 7; 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.
- The exam is **open book!** All kinds of material are permitted (access to Internet, access to your course notes, etc.).
- The exam is **online**. You access it on **Learn**. The link to the exam will be displayed at the top of the main page of the course.
- Date: **2 November 2021**
- Time: from 2:30pm to 5:30pm (3 hours)

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 answered 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`