Lab Timetable and Information
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.

2 Course structure

There is 1 lab per week, with 3 options:

- Tuesday, 16:00–18:00, Jack Erskine 136 Lab 4.
- Wednesday, 14:00–16:00, Jack Erskine 136 Lab 1.
- Friday, 16:00–18:00, Jack Erskine 136 Lab 4.

Labs take place in Jack Erskine 136 Lab 1 or 4. It is **highly recommended** to attend each lab session. The teaching assistant (Ryan) will mark your presence and participation to weekly lab sessions. Presence and fair participation to labs give you full mark.

However, in case of any unfortunate events (e.g. being sick), labs can be done online. In return, a report of the lab, done remotely, will be requested, along with a **justification of student absence**. The report contains your answers to the questions of the lab sheet. You are asked to submit your report by email, sent to both the lecturer and teaching assistant (see contact details at the end of the document). The report should be sent within one week after the missed lab:

- e.g. if you miss your weekly lab on **Friday 6 August**, then you should send the report by **Friday 13 August**.

If you do not send any report, or you send it after the due date, then you will not obtain the full mark allocated for labs. Note that if you attend the labs, then you do not need to submit a report!

3 labs require to use the open-source CrypTool 2 software (a free software but full of bugs, unfortunately!). In case you must to those labs remotely, please check the website `https://www.cryptool.org/en/` to download its second version (CrypTool 2).

Exercises/questions may not be all covered during their lab session. Solutions/answers will be posted to LEARN aftrer the corresponding labs:

- e.g. for lab sessions running on Week 2 (26-30 July), solutions/answers will be posted Week 4 (9-13 August), after the deadline for those who have done the lab remotely has passed.

Feel free to have a chat with the lecturer and/or teaching assistant if you have questions and concerns about labs.

2.1 Term 1 Plan

Week starting date	Course week	Monday lecture	Thursday lecture	Lab
19/07/2021	1	L1: Course introduction	L2: Course overview	no lab
26/07/2021	2	L3: Discrete mathematics	L4: CrypTool (at home)	Lab 1: Introduction
02/08/2021	3	L5: Classical encryption part 1	L6: Classical encryption part 2	Lab 2: Discrete maths exercises
09/08/2021	4	L7: Block ciphers	L8: Block cipher modes	Lab 3: CrypTool part 1
16/08/2021	5	L9: Stream ciphers	L10: Number theory	Lab 4: CrypTool part 2
23/08/2021	6	L11: Hash functions and MACs	L12: Public key crypto part 1	Lab 5: Number theory exercises

2.2 Term 2 Plan

Week starting date	Course week	Monday lecture	Thursday lecture	Lab
13/09/2021	7	L13: Public key crypto part 2	L14: Digital signatures	Lab 6: Hash functions and MACs exercises
20/09/2021	8	L15: PKI and certificates	L16: Key establishment	Lab 7: CrypTool part 3
27/09/2021	9	L17: TLS part 1	L18: TLS part 2	Lab 8: PKI and certificates
04/10/2021	10	no lecture	no lecture	Lab 9: Digital signatures and key establishment exercises
11/10/2021	11	L19: IPSec and VPN	L20: Email security	Lab 10: TLS
18/10/2021	12	L21: Malware and attacks	L22: Recap lecture	Lab 11: IPSec and email security exercises

2.3 Release dates of Labs sheet containing the answers.

Since labs run over the entire week, and since you have one week to submit your report in case you were absent, then there are 2 weeks between releasing the labs' questions and releasing the labs' answers.

Lab	Answer release date
Lab 1: Introduction	09/08/2021
Lab 2: Discrete maths	16/08/2021
Lab 3: CrypTool part 1	23/08/2021
Lab 4: CrypTool part 2	30/08/2021
Lab 5: Number theory	06/09/2021
Lab 6: Hash functions	27/09/2021
Lab 7: CrypTool part 3	04/10/2021
Lab 8: PKI and certificates	11/10/2021
Lab 9: Digital signatures and key establishment	18/10/2020
Lab 10: TLS	25/10/2020
Lab 11: IPSec and email security	01/11/2021

2.4 More information about labs!

- You may not finish the lab questions/exercises on time, by the end of your lab session, and it is totally fine. Most of the labs are about exploring, not performing and having results. Therefore, you must focus on the lab tasks of the current week and not the ones of previous weeks; otherwise, you will be far behind the schedule. For instance, for Week 4 (starting on Monday 09 August), you have to work on the questions of Lab 3, and not the ones of Labs 1 and 2.

- Most of the lab contents are not included in the exam syllabus. So do not spend too much time on those labs. They are here to explore and observe cryptographic items. CrypTool is a great software to look at old and current ciphers but there are many bugs, and that's annoying for everyone! Labs on PKI and TLS are a great introduction to those concepts, however, this is just the "surface".

- Labs 1, 2, 6, 7, 9 and 11 are part of the exam syllabus. However, if you do not finish them on time (i.e. by the end of your lab session), that's ok. You can keep on at home, before or after the answers are uploaded to Learn. If you have questions about them, feel free to ask me and Ryan.

- If you are stuck on one question for too long (regarding your own estimate), then chat with other students in your lab group, who may have found the solution, or chat with the teaching assistant, or move on to the next questions. I highly encourage discussing and sharing during labs; in real life, work will be team-based rather than individual!

- I agree that answers are uploaded late and that's not ideal to review the lab questions. I give the possibility for those who cannot attend the labs to still work on them as other students. However, I ensure that all answers will be released well before the exam takes place.

2.5 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`