# 50.020 Security Class Calendar (Year 2019)

**Notes: Class time (Week 1-Week 13):**

- Session 1: Monday 1:30-3pm
- Session 2: Tuesday 1:30-3pm
- Session 3: Thursday 1-3pm

**Quick facts:**

For **week 14**, there is one session on Thursday (30 April) 10:30am-12pm.

**Mid-term exam** on Week 6 Thursday 1:30-3pm.

**Final exam** on Week 14 Friday 9-11am.

**Team project: CTF (Capture the Flag)** on Weeks 9-11 (Labs 7-9).

**10 labs**= 7 labs + CTF (equivalent to 3 labs)

Two **guest lectures**: Week 9 Wednesday and Week 13 (including CTF prize award). Both are compulsory.

| Week | Dates | Topic | Remarks |
|---|---|---|---|
| **1** | (Monday) 28 Jan +<br>(Tuesday) 29 Jan<br><br>(Thursday) 31 Jan | Intro + OTP<br><br>Lab 1: Intro + Shiftciphers | |
| **2** | 4 Feb +<br><br>**5 Feb**<br><br>7 Feb | Hash Functions +<br><br>**CNY NO CLASS**<br><br>Lab 2: Cipher Breaking | |
| **3** | 11 Feb+ 12 Feb<br><br>14 Feb | Hash Applications<br>Passwords and Rainbow Tables<br><br>Lab 3: Hashes and Rainbow Tables | |
| **4** | 18 Feb + 19 Feb<br><br>21 Feb | Web Security (Part I)<br>Web Security (Part II)<br><br>Lab 4: Web Security | |
| **5** | 25 Feb+ 26 Feb | OS Security 1 +<br>Buffer overflow Attacks | |

| | | | |
|---|---|---|---|
| | 28 Feb | Lab 5: Buffer overflow | |
| **6** | 4 Mar +5 Mar<br><br>7 Mar | OS Security 2 +<br>Mid-term Recap<br><br>Lab time: Mid-term exam (1.5 hr hour exam, so tentatively 1:30-3pm) | The last 1.5hr lab time is used for Mid-term exam, while the first 0.5 hr can be used for preparation |
| **7** | **(Monday) 11 Mar** | **Recess Week** | **No class** |
| **8** | 18 Mar + 19 Mar<br><br>21 Mar | Mar 18: Block Cipher<br>+ Modular Arithmetics (Part I)<br><br>Lab 6: Present | Announce CTF instructions earlier: in Week 8, to give students more time for CTF |
| **9** | 25 Mar + 26 Mar<br><br>27 March 1-3pm<br><br>28 Mar | Modular Arithmetics (Part II)<br><br>Guest Lecture from ST Engineering (compulsory for Security students.)<br><br>Lab 7: CTF Part 1: Challenge Draft | Students submit CTF challenge drafts for instructors' feedback<br><br>Students can polish their challenge based on instructors' comments. |
| **10** | 1 April + 2 April<br><br>4 April | Key establishment + Public Key Cryptography<br><br>Lab 8: CTF Part 2: Challenge Finalized | CTF challenges: once finalized, all teams open their challenges to other groups for solving.<br>Other teams have around 1 week time to solve the challenges. |
| **11** | 8 April + 9 April<br><br>11 April | Side-channel Attacks +<br>Digital Signatures<br><br>Lab 9: CTF Part 3: finalize CTF challenge solutions, Placeholder for CTF challenges, Challenges Vote | |
| **12** | 15 April + 16 April<br><br>18 April | NS and TLS +<br>Bitcoin<br><br>Lab 10: TLS + ARP spoofing | |
| **13** | 22 April + 23 April | Zero knowledge protocol<br>+ final recap | |

| | | | |
|---|---|---|---|
| | 25 April | Lab time: no new lab, but CitiBank guest lecture + CTF prize award | |
| **14** | 29 April<br><br>30 April class: 10:30am-12pm<br><br>3 May Fri: Exam | 29 April NO class<br><br>30 April class: 10:30am-12pm, for consultation.<br><br>3 May Fri: Final Exam (9-11 am) | |