



## Prescription

Cryptographic mechanisms are widely deployed for communication and data protection. This course addresses how cryptographic mechanisms can be effectively used within larger security systems and how cryptographic mechanisms can be vulnerable in deployed systems. Topics covered include cryptographic primitives, cryptographic protocols, cryptanalytic techniques on primitives and protocols in deployed systems and attacks based upon common errors in use of libraries. Practical work will include best practice use of cryptographic libraries and attacks.

## Course learning objectives

Students who pass this course will be able to:

1. Describe the security properties and different application areas of common cryptographic primitives and protocols.
2. Analyse, evaluate and correctly use the most appropriate cryptographic libraries to implement specified data protection requirements or security protocols.
3. Use cryptanalytic techniques and tools to analyse and identify security vulnerabilities in the implementation of data protection and security protocols.

## Withdrawal from Course

Withdrawal dates and process:

<https://www.wgtn.ac.nz/students/study/course-additions-withdrawals>

## Lecturers

### Ian Welch (Coordinator)

ian.welch@vuw.ac.nz 04 4635664

131 Alan MacDiarmid Bldg Gate 7 Kelburn Pde, Kelburn

### Harith Al-Sahaf

harith.al-sahaf@vuw.ac.nz 04 4635656

129 Cotton, Kelburn

## Teaching Format

This course will be offered in-person and online. For students in Wellington, there will be a combination

of in-person components and web/internet based resources. It will also be possible to take the course entirely online for those who cannot attend on campus, with all the components provided in-person also made available online.

There are two lectures per week that will be recorded and starting from week four there will be weekly helpdesks will be both in person and provided over Zoom.

## Student feedback

This is the first time we have run the course so there is no feedback to report upon.

## Dates (trimester, teaching & break dates)

- Teaching: 13 July 2020 - 18 October 2020
- Break: 17 August 2020 - 30 August 2020
- Exam period: 19 October 2020 - 25 October 2020

## Class Times and Room Numbers

### 13 July 2020 - 16 August 2020

- **Monday** 12:00 - 12:50 – LT119, Hunter, Kelburn
- **Thursday** 15:10 - 16:00 – LT220, Murphy, Kelburn

### 31 August 2020 - 18 October 2020

- **Monday** 12:00 - 12:50 – LT119, Hunter, Kelburn
- **Thursday** 15:10 - 16:00 – LT220, Murphy, Kelburn

## Set Texts and Recommended Readings

### Required

The textbook for the course is:

- *Cryptography Engineering: Design Principles and Practical Applications* 1st Edition by Niels Ferguson (Author), Bruce Schneier and Takayoshi Kohno

## Mandatory Course Requirements

In addition to achieving an overall pass mark of at least 50%, students must:

- Achieve at least a **D** in the take home test, because the test assesses understanding of concepts and what was learnt in assignments independently.

*If you believe that exceptional circumstances may prevent you from meeting the mandatory course requirements, contact the Course Coordinator for advice as soon as possible.*

## Assessment

The assignments will apply theory learnt in the lectures while the take home test will be related to the lecture material and learning during the assignments. The take home test will be related to the lecture material and learning during the assignments.

Assessment Item	Due Date or Test Date	CLO(s)	Percentage
Implementation assignment (5 weeks).	06/09/20	CLO: 1	40%
Analysis assignment (5 weeks).	11/10/20	CLO: 2	40%
Take home test (24 hours).	Assessment week	CLO: 1,2,3	20%

## Penalties

Late assignment submissions will receive a penalty of 10% for each day late (pro-rata).

## Extensions

Each student will have three "late days" which you may choose to use for any assignment or assignments during the course. There will be no penalty applied for these late days. You do not need to apply for these, instead any late days you have left will be automatically applied to assignments that you submit late.

## Submission & Return

All work is submitted through the ECS submission system, accessible through the course web pages. Marks and comments will be returned through the ECS marking system, also available through the course web pages.

## Workload

The total workload for CYBR 371 is 150 hours. In order to maintain satisfactory progress in CYBR 231, you should plan to spend an average of 10 hours per week on this course. An approximate breakdown is: lectures 2 hours, assignments 5 hours and assigned readings/review of notes 2 hours.

## Teaching Plan

See: [https://ecs.wgtn.ac.nz/Courses/CYBR372\\_2020T2/LectureSchedule](https://ecs.wgtn.ac.nz/Courses/CYBR372_2020T2/LectureSchedule)

## Communication of Additional Information

All online material for this course can be accessed at [https://ecs.wgtn.ac.nz/Courses/CYBR372\\_2020T2/](https://ecs.wgtn.ac.nz/Courses/CYBR372_2020T2/).

## Links to General Course Information

- Academic Integrity and Plagiarism: <https://www.wgtn.ac.nz/students/study/exams/integrity-plagiarism>
- Academic Progress: <https://www.wgtn.ac.nz/students/study/progress/academic-progress> (including restrictions and non-engagement)
- Dates and deadlines: <https://www.wgtn.ac.nz/students/study/dates>
- Grades: <https://www.wgtn.ac.nz/students/study/progress/grades>
- Special passes: Refer to the Assessment Handbook, at <https://www.wgtn.ac.nz/documents/policy/staff-policy/assessment-handbook.pdf>
- Statutes and policies, e.g. Student Conduct Statute: <https://www.wgtn.ac.nz/about/governance/strategy>

- Student support: <https://www.wgtn.ac.nz/students/support>
- Students with disabilities: [https://www.wgtn.ac.nz/st\\_services/disability/](https://www.wgtn.ac.nz/st_services/disability/)
- Student Charter: <https://www.wgtn.ac.nz/learning-teaching/learning-partnerships/student-charter>
- Terms and Conditions: <https://www.wgtn.ac.nz/study/apply-enrol/terms-conditions/student-contract>
- Turnitin: <http://www.cad.vuw.ac.nz/wiki/index.php/Turnitin>
- University structure: <https://www.wgtn.ac.nz/about/governance/structure>
- VUWSA: <http://www.vuwsa.org.nz>

**Offering CRN:** [32078](#)

**Points:** 15

**Prerequisites:** CYBR 171; CYBR 271 or COMP 261; NWEN 243

**Duration:** 13 July 2020 - 25 October 2020

**Starts:** Trimester 2

**Campus:** Kelburn