

In Progress

Please note that this Unit Profile is still in progress. The content below is subject to change.



COIT13240 Applied Cryptography

Term 1 - 2025

Profile information current as at 12/02/2025 01:32 pm

All details in this unit profile for COIT13240 have been officially approved by CQUniversity and represent a learning partnership between the University and you (our student). The information will not be changed unless absolutely necessary and any change will be clearly indicated by an approved correction included in the profile.

General Information

Overview

In this unit, you will learn techniques for securing information and communications against adversaries, in particular with regards to confidentiality, integrity and authentication. Informed by the history of cryptography, you will learn the cryptographic primitives that are used to secure information today such as symmetric key encryption, message authentication codes, public key cryptography and digital signatures. You will also study future issues in cryptography, including the challenges raised by quantum computing. While you will learn and use basic mathematics, this unit will focus on cryptographic concepts relevant to cyber security specialists, rather than the mathematical underpinnings of the algorithms. This practical treatment of cryptography will be highlighted in laboratory tasks, where you will use software to attack and secure information in various realistic scenarios.

Details

Career Level: *Undergraduate*

Unit Level: *Level 3*

Credit Points: 6

Student Contribution Band: 8

Fraction of Full-Time Student Load: 0.125

Pre-requisites or Co-requisites

Pre-requisite: COIT12202 Network Security Concepts

Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the [Assessment Policy and Procedure \(Higher Education Coursework\)](#).

Offerings For Term 1 - 2025

- Brisbane
- Cairns
- Melbourne
- Online
- Rockhampton
- Sydney

Attendance Requirements

All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

Website

[This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.](#)

Class and Assessment Overview

Recommended Student Time Commitment

Each 6-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 hours for the unit.

Class Timetable

[Regional Campuses](#)

Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

[Metropolitan Campuses](#)

Adelaide, Brisbane, Melbourne, Perth, Sydney

Assessment Overview

1. **In-class Test(s)**

Weighting: 30%

2. **Written Assessment**

Weighting: 25%

3. **Project (applied)**

Weighting: 45%

Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the [University's Grades and Results Policy](#) for more details of interim results and final grades.

CQUniversity Policies

All University policies are available on the [CQUniversity Policy site](#).

You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the [CQUniversity Policy site](#).

Previous Student Feedback

Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

Feedback from Student evaluations

Feedback

Tests are stressful due to level of difficulty, high stakes, and variety of topics covered in short time.

Recommendation

Reduce the weight of the tests in the unit, adding more focus on the practical activities in the project and journal.

Feedback from Student evaluations

Feedback

The quality of the learning materials was appreciated, however the time needed to study the content covered is high.

Recommendation

Continue with the diverse set of learning materials, but incorporate more guidance on depth of understanding needed of each topic, e.g. via more quiz questions for self-assessment.

Feedback from Unit Coordinator reflection

Feedback

Active use of GitHub and Teams for group work usually leads to higher quality project outcomes.

Recommendation

Demonstrate the benefits of GitHub and Teams for teamwork early in the term and allocate more marks to their use for the project.

Unit Learning Outcomes

On successful completion of this unit, you will be able to:

1. Discuss principles used to design secure cryptographic algorithms
2. Explain the operation of attacks on cryptographic algorithms
3. Compare the strengths and weaknesses of different cryptographic algorithms and their implementations
4. Design secure information services using a variety of cryptographic algorithms.

The Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments and individuals in many countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles. ACS members can use the tool [MySFIA](#) to build a skills profile.

This unit contributes to the following workplace skills as defined by [SFIA 9](#) (the SFIA code is included)

- Information Security (SCTY)
- Security Administration (SCAD)
- Specialist Advice (TECH)
- Information Assurance (INAS)
- Vulnerability Assessment (VUAS)
- Infrastructure Design (IFDN)
- Threat Intelligence (THIN)
- Infrastructure Operations (ITOP)

The National Initiative for Cybersecurity Education ([NICE](#)) Framework defines knowledge, skills and tasks needed to perform various cyber security roles. Developed by the National Institute of Standards and Technology (NIST), the NICE Framework is used by organisations to plan their workforce, including recruit into cyber security positions.

This unit helps prepare you for roles such as Systems Security Analyst, Network Operations Specialist and Systems Administrator, contributing to the following knowledge and skills:

- K0005 Knowledge of cyber threats and vulnerabilities.
- K0018 Knowledge of encryption algorithms
- K0019 Knowledge of cryptography and cryptographic key management concepts
- K0053 Knowledge of measures or indicators of system performance and availability.
- K0071 Knowledge of remote access technology concepts.
- K0075 Knowledge of security system design tools, methods, and techniques.
- K0201 Knowledge of symmetric key rotation techniques and concepts.
- K0318 Knowledge of operating system command-line tools.
- K0622 Knowledge of controls related to the use, processing, storage, and transmission of data.
- S0040 Skill in implementing, maintaining, and improving established network security practices.
- S0060 Skill in writing code in a currently supported programming language (e.g., Java, C++).
- S0077 Skill in securing network communications.

Alignment of Learning Outcomes, Assessment and Graduate Attributes



Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes			
	1	2	3	4
1 - In-class Test(s) - 30%	•	•		
2 - Written Assessment - 25%	•	•	•	
3 - Project (applied) - 45%			•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes			
	1	2	3	4
1 - Communication	•	•	•	•
2 - Problem Solving	•	•	•	•
3 - Critical Thinking	•	•	•	•
4 - Information Literacy	•	•	•	•
5 - Team Work				•
6 - Information Technology Competence	•	•	•	•
7 - Cross Cultural Competence				
8 - Ethical practice			•	•
9 - Social Innovation				
10 - Aboriginal and Torres Strait Islander Cultures				

Textbooks and Resources

Information for Textbooks and Resources has not been released yet.

This information will be available on Monday 17 February 2025

Academic Integrity Statement

Information for Academic Integrity Statement has not been released yet.

This unit profile has not yet been finalised.