# COIT13240 *Applied Cryptography*

## Term 1 - 2024

Profile information current as at 29/07/2024 04:00 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 - 2024

- Cairns
- Online

### 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: 40%
2. **Written Assessment**
Weighting: 20%
3. **Project (applied)**
Weighting: 40%

### 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 Feedback, including Unit Evaluation

**Feedback**

New concepts and tools to learn each week, combined with regular journal entries and multiple tests, leaves little time for an in-depth understanding of topics.

**Recommendation**

Reduce the number of tests during the term, and make it clearer that during busy weeks (e.g., when tests are held, key points in a project) the journal entries can focus on reflections on the test and project.

### Feedback from Unit Evaluation and Unit Coordinator Reflection

**Feedback**

The connection between the ciphers and skills learnt in this unit and the technologies graduates will work with is not clear.

**Recommendation**

Include more activities on cryptography for web technologies in the project, and include a task towards the end of the term for reflecting on the relevance of the learnt knowledge/skills to future jobs.

## 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 7 (the SFIA code is included)

- Information Security (SCTY)
- Security Administration (SCAD)
- Specialist Advice (TECH)

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

— N/A Level • Introductory Level • Intermediate Level • Graduate Level ◦ Professional Level ◦ Advanced Level

### Alignment of Assessment Tasks to Learning Outcomes

| Assessment Tasks | Learning Outcomes | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1 - In-class Test(s) - 40% | • | • | • | • |
| 2 - Written Assessment - 20% | • | • | | |
| 3 - Project (applied) - 40% | | | • | • |

### 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

### Textbooks

COIT13240

**Prescribed**

**Cryptography and Network Security: Principles and Practice**
7th Edition (2017)
Authors: William Stallings
Pearson
ISBN: 9781292158594
Binding: eBook

### IT Resources

**You will need access to the following IT resources:**

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- Wireshark
- Zoom Video Conference Application
- Python
- Github.com Account
- Linux or Unix Operating System
- Microsoft Teams

## Referencing Style

All submissions for this unit must use the referencing style: Harvard (author-date)
For further information, see the Assessment Tasks.

## Teaching Contacts

**Steven Gordon** Unit Coordinator
s.d.gordon@cqu.edu.au

## Schedule

**Week 1 - 04 Mar 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Cryptography Concepts and Tools | Cryptography and Network Security, 7th Ed, by William Stallings: Chapter 1 | |

**Week 2 - 11 Mar 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Classical Ciphers | Stallings: Chapter 3 | |

**Week 3 - 18 Mar 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Encryption and Attacks | Stallings: Chapter 4 | |

**Week 4 - 25 Mar 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Block Ciphers in Practice | Stallings: Chapter 4, 6 and 7 | Test 1 (in tutorial class) |

**Week 5 - 01 Apr 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Public Key Crypto and RSA | Stallings: Chapters 9 and 2 | Draft Journal due Week 5 Tuesday 2 April 2024 9:00 AM AEST |

**Vacation Week - 08 Apr 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|

**Week 6 - 15 Apr 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Other Public-Key Cryptosystems | Stallings: Chapter 10 | |

**Week 7 - 22 Apr 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Public Key Crypto in Practice | Online Readings | |

**Week 8 - 29 Apr 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Hash Functions and MACs | Stallings: Chapter 11 and 12 | Test 2 (in tutorial class) |

**Week 9 - 06 May 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Authentication and Data Integrity | Stallings: Chapter 13 | |

**Week 10 - 13 May 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Authentication in Practice | Online Readings | Full Journal due Week 10 Tuesday 14 May 2024 9:00 AM AEST |

**Week 11 - 20 May 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Project Presentations | - | Project Presentations (in class) |

**Week 12 - 27 May 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Quantum Computing and Cryptography | Online Readings | Test 3 (in tutorial class) |

**Review/Exam Week - 03 Jun 2024**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| No class | - | Project due Week 13 Tuesday 4 June 2024 9:00 AM AEST |

## Term Specific Information

You are expected to use GitHub for your journal and project. You will need to create an account (if you do not already have one) and use GitHub Classroom. Instructions for doing so will be provided on Moodle.

GitHub is a website that may be hosted overseas (including the United States). In setting up an account and using for your journal and project, you will be transferring personal information to GitHub. While there is some risk in transferring your personal information overseas, we believe the benefits to you far outweigh the risk. You will gain experience using a tool widely used in industry, you will have access to tools for version control, backup, and collaboration on your resources, and will have artefacts to show to potential employers. If you have concerns with using GitHub, please contact the Unit Coordinator to discuss options (such as setting up your own Git server).

You are required to use Microsoft Teams for communications, including within your group in the project. Microsoft Teams is a supported CQUniversity online service, as such you do not have an option of using another communications platform.

## Assessment Tasks

### 1 In-Class Tests

**Assessment Type**
In-class Test(s)

**Task Description**
You will undertake three (3) in-class tests on Moodle throughout the term. Each test will cover topics from the weeks leading up to that test, and may include questions similar to earlier tests. Each test will consist of multiple-choice questions, short or long answer questions and/or calculations. Some questions may require the use of software and online systems (e.g. GitHub). There will be multiple independent questions in each test. All tests are individual assessment.
Each test will be time limited, typically allowing you between 30 and 60 minutes to complete the test. Some tests may be longer. Test time limits, topics, and open/close times can be found on Moodle.
The tests must be taken during your allocated timeslot: either the tutorial or, in special cases, a designated time negotiated in advance with the Unit Coordinator. The test will open shortly after the start of your time slot and will close after the time limit has been reached. You will be allowed only a single attempt at each test, with the score for that attempt counting towards your grade.
Tests will be held during the weeks: 4, 8 and 12. Tests will be supervised. Tests will be open book. You are not allowed to communicate with anyone (including other students or people online) while the test is open.
You will not be allowed to take a test at any time outside of your allocated timeslot, unless an Assessment Extension Request is approved. The test will close at the same time for all students in your timeslot. If you arrive late for the timeslot, you will not be granted extra time. Changes to test times can only be granted with approval by the Unit Coordinator.
For those in online tutorials, you will need access to a webcam, speakers and microphone (e.g., headset).
You are assumed to have a working computer and Internet connection during term, and especially during times when attempting a test. Technical problems, such as a computer crash or loss of Internet connection, will not usually be a reason for an extra attempt or extension. You are expected to prepare your computer before the test starts. If problems outside of your control occur during a test, report immediately to your tutor, who may either extend the time or allow you to undertake the test at another time (with the Unit Coordinator's approval).

**Assessment Due Date**

See the task description.

**Return Date to Students**

One week after the test

**Weighting**
40%

**Assessment Criteria**
Test 1 and 2 are worth 10% each; Test 3 is worth 20%.
In most cases, test answers will be automatically marked, with marks awarded based on the correctness of the answer within the context of topics covered in unit. Questions may be worth different marks, with the marks shown in the test. If test answers are manually marked (e.g., explanation style questions), then marks will be awarded based on the correctness and clarity of the answer.
As results and solutions may be released shortly after the due date, late submissions are not accepted. Making no attempts before the due date will result in a score of 0.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Learning Outcomes Assessed**

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

## 2 Journal

**Assessment Type**
Written Assessment

**Task Description**
You will keep a journal throughout the unit that captures your workings, insights and reflections on each topic. For example, as you learn about a new cipher, your will record your own workings and examples in the journal, you will compare the cipher design to others, and you will explore possible attacks on that cipher (and/or explain why some attacks are unsuccessful).
The journal is expected to be maintained each week. Examples of content that may be included are:

- Photos of manual (paper) calculations for simple classical ciphers,
- Diagrams illustrating attacks on ciphers, with explanation of why they are (not) successful,
- Code segments that you used in testing a modern cipher,
- Explanations of difficulties you had in understanding a cipher and/or its relation to others,
- Links to and short summaries of websites/papers/software on ciphers and their attacks,
- Challenges encountered and insights gained from implementing and applying ciphers, i.e. in the Security Project.

You will have to maintain your journal such that there is evidence of regular contributions. Your journal must be created in a GitHub repository created using GitHub Classroom. As this is your own journal, you should not share with other students. The journal should use basic Markdown formatting (using just plaintext or uploading a Word document is insufficient). Details of creating the GitHub repository can be found on Moodle.
You are required to submit your journal early in the term (Draft Journal) so you can gain feedback on the suitability of your entries so far. The entire journal is then submitted towards the end of term (Full Journal).

**Assessment Due Date**

Draft Journal due Week 5 Tuesday 2 April 2024 9:00 AM AEST; Full Journal due Week 10 Tuesday 14 May 2024 9:00 AM AEST

**Return Date to Students**

Draft Journal two weeks after submission; Full Journal on Certification of Grades day

**Weighting**
20%

**Assessment Criteria**
The journal is an individual assessment worth 20% of the unit assessment. The Draft Journal, which contains only entries for the first several weeks, is worth 5%; the Full Journal, which contains entries for all weeks up until deadline, is worth 15%. If you submit the draft journal before the deadline, make a genuine attempt in the draft, and then make substantial improvements based on feedback, then your mark for the Draft Journal may increase when the Full Journal is marked.
Your journal will be assessed on:

- Quality of contributions. E.g., the entries are clear, correct and demonstrate understanding of the topics covered, including progressive learning/improvement over the weeks and reflections on learning.
- Novel insights. E.g., you provide insights or explanations that go beyond what is covered in the unit material.
- Regular, relevant, professional contributions. E.g., there are entries each week (as opposed to all added at the end of term), and those entries are relevant to the current topics in the unit. The journal must be maintained in a private GitHub repository shared only with the Unit Coordinator. The journal should use basic Markdown formatting; using just plaintext or upload a Word document to GitHub is insufficient.

While the journal will be maintained on GitHub, you must also submit a ZIP of the journal on Moodle before the deadline. The ZIP file can easily be produced by exporting the repository in GitHub. This is necessary so that a permanent record of your contribution is available in Moodle (in case the online platform is not available in the future).

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Learning Outcomes Assessed**

- Discuss principles used to design secure cryptographic algorithms
- Explain the operation of attacks on cryptographic algorithms

## 3 Security Project

**Assessment Type**

Project (applied)

**Task Description**

This project involves you developing and applying a set of cryptographic tools, as well as analysing security issues and attacks.

Some questions/parts will require you to investigate beyond what is covered in the unit lecture/tutors. You may need to read and summarise research papers, standards, technical reports, and websites. Some questions/parts may require you to write software to complete a task. Your software must be implemented in Python. While examples of Python will be used during the unit, you may be required to learn advanced features to complete the software.

The project will be a mix of group work and individual work. You will be required to form a group and complete some tasks together. You will also be required to complete some tasks on your own. Aspects of the project, especially the software, may be discussed in class and on Microsoft Teams. Each group will have a Teams channel that must be used for group communication. The Unit Coordinator will facilitate/moderate discussion about the project (including the group Teams channel).

You will be required to use GitHub to track your software development and document your project. Therefore, you will need an account on GitHub. The use of an online collaborative software tracking tool will allow regular feedback on your progress and sharing of code when appropriate. The details of using GitHub repositories and sharing code will be specified on Moodle. While your software and documentation will be stored on GitHub, you will still be required to submit files on Moodle when the assessment is due (e.g., export a Zip of the repository and upload to Moodle). This is necessary so that a permanent record of your contribution is available in Moodle (in case the online platform is not available in the future).

You will be required to give a presentation about your project. The presentation will be an opportunity for verbal feedback on progress; you will have an opportunity to make improvements after the presentation. If you do not satisfactorily explain your contributions to the project in the initial presentation, then you may be asked to give another presentation after submission of the project.

**Assessment Due Date**

Presentation in Week 11; Project due Week 13 Tuesday 4 June 2024 9:00 AM AEST

**Return Date to Students**

Certification of Grades day

**Weighting**

40%

**Minimum mark or grade**

35% of the Security Project total (14 out of 40)

**Assessment Criteria**

The project will be marked based on the quality and technical depth of the solution(s), as well as the ability to collaborate with others to arrive at the solution. A detailed marking guide, with weights for each part, will be provided on Moodle.

A part of your mark will be for group work, and the remaining will be individual. Note that even for group work, each member of the group may receive different marks.

The presentation is a required for the project. The mark for your project will be based on a combination of your presentation, any written reports, collaborative tool data (e.g. GitHub logs), and submitted artefacts (e.g. code, data files). If you do not present, then you cannot score more than 13 marks out of 40 for the project.

Several tasks may require you to design, implement and test features in Python. For these tasks, you will mainly be marked on your submitted code, however you also receive some marks for a brief explanation and demonstration of operation (e.g., test results). Submitting code that does not work (or not submitting any code) will usually result in 0 marks for that part, irrespective of the explanation and test results.

The primary criterion for assessing any code is functionality. That is, does it correctly do what it is supposed to do? Clarity of the code is also important, i.e., is the operation and code structure clear and easy to follow? Preference is for clarity over efficiency (e.g. run-time efficiency, coding efficiency).

**Referencing Style**

- Harvard (author-date)

**Submission**

Online Group

**Learning Outcomes Assessed**

- Compare the strengths and weaknesses of different cryptographic algorithms and their implementations
- Design secure information services using a variety of cryptographic algorithms.

## Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the **Student Academic Integrity Policy and Procedure**. This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

**What is a breach of academic integrity?**
A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

**Why is academic integrity important?**
A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

**Where can I get assistance?**
For academic advice and guidance, the Academic Learning Centre (ALC) can support you in becoming confident in completing assessments with integrity and of high standard.

**What can you do to act with integrity?**

**Be Honest**

If your assessment task is done by someone else, it would be dishonest of you to claim it as your own

**Seek Help**

If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)

**Produce Original Work**

Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem