COIT13240 *Applied Cryptography*
Term 1 - 2020

Profile information current as at 04/05/2024 12:00 pm

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 - 2020

- Brisbane
- Melbourne
- Online
- 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: 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.

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)

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	•	•	•	•

Graduate Attributes	Learning Outcomes			
	1	2	3	4
7 - Cross Cultural Competence				
8 - Ethical practice			•	•
9 - Social Innovation				
10 - Aboriginal and Torres Strait Islander Cultures				

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes									
	1	2	3	4	5	6	7	8	9	10
1 - In-class Test(s) - 40%	•	•	•	•		•				
2 - Written Assessment - 20%	•	•	•	•		•				
3 - Project (applied) - 40%	•	•	•	•	•	•		•		

Textbooks and Resources

Textbooks

COIT13240

Prescribed

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

Additional Textbook Information
Copies can be purchased at the CQUni Bookshop here: http://bookshop.cqu.edu.au (search on the Unit code)

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

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

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 - 09 Mar 2020

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

Week 2 - 16 Mar 2020

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

Week 3 - 23 Mar 2020

Module/Topic	Chapter	Events and Submissions/Topic
Classical Ciphers	Stallings: Chapter 3	Test 1

Week 4 - 30 Mar 2020

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

Week 5 - 06 Apr 2020

Module/Topic	Chapter	Events and Submissions/Topic
Block Ciphers: DES, AES and others	Stallings: Chpaters 6, 7 and 8	Test 2

Vacation Week - 13 Apr 2020

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 20 Apr 2020

Module/Topic	Chapter	Events and Submissions/Topic
Public Key Cryptography	Stallings: Chapters 9 and 2	

Week 7 - 27 Apr 2020

Module/Topic	Chapter	Events and Submissions/Topic
RSA	Stallings: Chapter 9	Test 3

Week 8 - 04 May 2020

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

Week 9 - 11 May 2020

Module/Topic	Chapter	Events and Submissions/Topic
Hash Functions and MACs	Stallings: Chapters 11 and 12	Test 4

Week 10 - 18 May 2020

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

Week 11 - 25 May 2020

Module/Topic	Chapter	Events and Submissions/Topic
Key Management	Stallings: Chapter 14	Test 5

Week 12 - 01 Jun 2020

Module/Topic	Chapter	Events and Submissions/Topic
Advances in Cryptography	Online Readings	

Review/Exam Week - 08 Jun 2020

Module/Topic	Chapter	Events and Submissions/Topic
		Journal Due: Review/Exam Week Monday (8 June 2020) 9:00 am AEST **Security Project** Due: Review/Exam Week Monday (8 June 2020) 9:00 am AEST

Exam Week - 15 Jun 2020

Module/Topic	Chapter	Events and Submissions/Topic

Term Specific Information

This unit is delivered via a workshop each week. The unit content has new concepts and theory, as well as practical activities. You are recommended to use the workshop to discuss concepts and theory, and conduct practical activities. Therefore you should complete any readings, watch designated videos, and/or undertake practice quizzes before the workshop.
The unit also uses mathematics and software (i.e. Python programming language) that you may not be familiar with. While resources are provided to gain sufficient familiarity to complete the unit, a positive attitude is also recommended. For example, if you don't have a strong mathematical background, don't be put off: with some patience and practice, you will find the math relatively easy and even interesting.

Assessment Tasks

1 In-Class Tests

Assessment Type
In-class Test(s)

Task Description
You will undertake five (5) in-class tests on Moodle throughout the term. Each test will cover topics from the weeks leading up to that test. Each test will consist of multiple choice questions, short answer questions and/or calculations. Some questions may require the use of software. There will be multiple independent questions in each test. All tests are individual assessment.
Each test will be time limited, typically allowing you between 15 and 30 minutes to complete the test. Test time limits, topics, and open/close times can be found on Moodle.
The tests must be taken during your allocated timeslot: either your assigned class (for on-campus students) or 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 test test, with the score for that attempt counting towards your grade.
Tests will be held during the weeks: 3, 5, 7, 9 and 11. Tests will be supervised. Tests will be closed book, but with a selection of resources allowed or made available. 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 students studying via distance (online), the Unit Coordinator will negotiate with you a time at which you can undertake a supervised test via Zoom screen sharing. Distance (online) students will therefore 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
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 indicated 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.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence

2 Journal

Assessment Type
Written Assessment

Task Description
You will maintain 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 be required to maintain your journal such that there is evidence of regular contributions, e.g. using GitHub, an online blog, or portfolio software.

Assessment Due Date
Review/Exam Week Monday (8 June 2020) 9:00 am AEST

Return Date to Students

Certification of Grades day

Weighting
20%

Assessment Criteria
The journal is an individual assessment. Your journal will be assessed on:

- Quality of contributions: 50% (10 out of 20). E.g. the entries are clear, correct and demonstrate understanding of the topics covered.
- Novel insights: 25% (5 out of 20). E.g. you provide insights or explanations that go beyond what is covered in the unit material.
- Regular, relevant contributions: 25% (5 out of 20). 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.

A detailed marking guide will be provided in Moodle.

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

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence

3 Security Project

Assessment Type
Project (applied)

Task Description
You will build a software application (or service) that uses a variety of cryptographic mechanisms (such as symmetric block ciphers, public key encryption and authentication). You will focus on applying existing cryptographic libraries and APIs to build secure applications, although you may need to implement some cryptographic algorithms yourself. While you will be required to implement a base set of features, you also have the freedom to select additional features to implement.
Your software should 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 require both individual work and team work. You will be individually responsible for developing the software. However, your software must interoperate with that of other students in the class. Therefore you must work in a team to agree upon methods to achieve interoperability (e.g. protocols, formats), and also to test interoperability.
Testing of your software, including interoperability testing with others, will primarily be conducted via demonstration. That is, during an agreed timeslot before the project deadline, you demonstrate and explain the functionality of your software, and show that it works successfully with other students' software.
Teams must be formed by the end of Week 4, with each team having a minimum of three (3) members. Re-arrangement of teams during the term, e.g. if a student is sick, will be at the discretion of the Unit Coordinator.
You will have to be available to communicate with your team members (e.g. via email or Zoom meetings), and demonstrate your software to others. Therefore you will need access to video conferencing capabilities, e.g. Zoom, headset, webcam.
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).

Assessment Due Date
Review/Exam Week Monday (8 June 2020) 9:00 am AEST

Return Date to Students

Certification of Grades day

Weighting
40%

Assessment Criteria
The outputs of the project will be: code, documentation and test results.

- The primary criteria for assessing the 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).
- The documentation will be assesed based upon clarity and completeness, e.g. does the documentation clearly explain all main aspects of the software?
- The testing will be assessed based on completeness and accuracy, e.g. do the test results demonstrate all features worked correctly?

Marking may be done by a mix of manual inspection of the submission (e.g. reviewing the code) and live demonstrations (e.g. viewing you demonstrate the software).
Group assessment will be applied to the interoperability testing and documentation of features that enable interoperability. All other components will be individually assessed. The split of marks between the group and individual is:

- Individual assessment: 80% (32 out of 40)
- Group assessment: 20% (8 out of 40)

A detailed marking guide will be provided in Moodle with the project specification.

Referencing Style

- Harvard (author-date)

Submission
Online

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.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Team Work
- Information Technology Competence
- Ethical practice

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