COMP2300

Applied Cryptography

Session 2, In person-scheduled-weekday, North Ryde 2024

School of Computing

Contents

Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

General Information

Unit convenor and teaching staff
Convenor and Lecturer
Hassan Asghar
hassan.asghar@mq.edu.au
Contact via Email

Lecturer
Xuyun Zhang
xuyun.zhang@mq.edu.au
Contact via Email

Credit points
10

Prerequisites
(COMP1010 or COMP125) and (DMTH137 or MATH1007 or DMTH237)

Corequisites

Co-badged status
COMP6300

Unit description
This unit provides an introduction to modern applied cryptography. It deals with the concepts and techniques behind cryptographic primitives, such as hash functions, symmetric-key ciphers, public-key cryptography and digital signatures. It then explains the concept of cryptanalysis before addressing important cryptographic protocols. The unit concludes with a review of existing applications including blockchain and cryptocurrencies, electronic voting schemes, executable code signing, full disk encryption, etc.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

ULO1: Explain the concepts and principles on which modern cryptography relies upon.

ULO2: Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.

ULO3: Decipher simple encrypted messages using a range of cryptanalysis methods.

ULO4: Apply cryptographic technologies and protocols to increase data security and protect privacy.

General Assessment Information

Late Assessment Submission Penalty

Students enrolled in Session based units with written assessments will have the following university standard late penalty applied. Please see https://students.mq.edu.au/study/assessment-exams/assessments for more information.

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. Submission time for all written assessments is set at 11:55 pm. A 1-hour grace period is provided to students who experience a technical concern.

For any late submission of time-sensitive tasks, such as scheduled tests/exams, performance assessments/presentations, and/or scheduled practical assessments/labs, students need to submit an application for Special Consideration.

Assessments where Late Submissions will be accepted

In this unit, late submissions will accepted as follows:

Assignments 1 and 2 – YES, standard late penalty applies

Module Exams 1, 2 and 3 - NO, unless Special Consideration is granted

Weekly tasks - NO

Hurdle Assessment

The weekly tasks, i.e., weekly quizzes, are the only hurdle assessment for this unit. There will be 10 weekly quizzes. You are required to **attempt** at least 6 of the 10 to pass the hurdle. Note that the hurdle is the attempt, not the marks obtained. For example, you may secure less than 50% masks in the quizzes, but you will still pass the hurdle if you have attempted 6 or more of them. This activity is a hurdle to ensure that you are regularly attending and keeping up with the lectures and workshops preceding the quizzes. There is no opportunity to resit the hurdle, as it only requires you to attempt the quizzes. In the rare event that you missed a couple of quizzes resulting in you failing the hurdle, please email the unit convenor and apply for special consideration.

Special Consideration

The Special Consideration Policy aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment.

- *Written Assessments and Module Exams:* If you experience circumstances or events that affect your ability to complete the assignments and module exams in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

- *Weekly quizzes:* To pass the unit you need to attempt 6 out of the 10 weekly quizzes. A Special Consideration should only be applied for if you miss more than four of the weekly quizzes.

Requirements to Pass this Unit

To pass this unit, you must:

- Achieve a total mark of 50% or more
- Attempt at least 6 out of the 10 weekly quizzies

Assessment Tasks

Name	Weighting	Hurdle	Due
Weekly Tasks	10%	Yes	11:55 pm on Sundays, weekly
Module Exam #1	20%	No	5:55 pm on Wednesday week 5
Assignment 1	15%	No	11:55 pm on Friday ending week 7
Module Exam #2	20%	No	5:55 pm on Wednesday week 9
Assignment 2	15%	No	11:55 pm on Friday ending week 12
Module Exam #3	20%	No	5:55 pm on Wednesday week 13

Weekly Tasks

Assessment Type [1]: Problem set
Indicative Time on Task [2]: 5 hours
Due: **11:55 pm on Sundays, weekly**
Weighting: **10%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Each week, a set of exercises will be available online. Some require written submissions, while some are multiple choice. Your solutions should be submitted electronically via iLearn before the deadline specified in the text.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.
- Decipher simple encrypted messages using a range of cryptanalysis methods.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Module Exam #1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **5:55 pm on Wednesday week 5**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 1 to 4.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.
- Decipher simple encrypted messages using a range of cryptanalysis methods.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **11:55 pm on Friday ending week 7**
Weighting: **15%**

This assignment deals with symmetric-key cryptography and is due on week 7. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign

messages.

- Decipher simple encrypted messages using a range of cryptanalysis methods.

Module Exam #2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **5:55 pm on Wednesday week 9**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 9 during practical class. This will test your understanding of material covered in weeks 5 to 8.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 8 hours
Due: **11:55 pm on Friday ending week 12**
Weighting: **15%**

This assignment deals with public-key cryptography and is due on week 12. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Module Exam #3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **5:55 pm on Wednesday week 13**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 13 during practical class. This will test your understanding of material covered in weeks 9 to 12.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

COMPUTING FACILITIES

Important! Please note that this is a BYOD (Bring Your Own Device) unit. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the workshop, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

CLASSES

Each week you should complete any assigned readings and review the lecture slides in order to prepare for the lecture. There are two hours of lectures and a one-hour workshop every week. The workshops have hands-on exercises to reinforce concepts introduced during the lectures; you should have chosen a practical on enrollment. You will find it helpful to read the workshop instructions before attending - that way, you can get to work quickly!

For details of days, times and rooms consult the timetables webpage.

Note that **Lectures and Workshops commence in week 1**.

METHODS OF COMMUNICATION

We will communicate with you via your university email or through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to the unit convenor from your university email address.

REQUIRED AND RECOMMENDED TEXTS AND/OR

MATERIALS

Required readings for this unit:

- N. Smart, **Cryptography Made Simple**, Springer. The PDF version of the book is available online at https://www.springer.com/us/book/9783319219356 and also through MQ Library.
- Easttom, Chuck. Modern Cryptography: Applied Mathematics for Encryption and Information Security. 1 edition. New York: McGraw-Hill Education, 2015. The book is available in online format through the Library; there will be allocated readings each week.

Recommended readings for this unit:

- A. J. Menezes, P. C. van Oorrschot and S. A. Vanstone, **Handbook of applied cryptography (HAC)**, CRC Press, Boca Raton, FL, 1996. All required chapters are available online at http://cacr.uwaterloo.ca/hac/

TECHNOLOGY USED AND REQUIRED

iLearn

iLearn is a Learning Management System that gives you access to lecture slides, lecture recordings, forums, assessment tasks, instructions for practicals, discussion forums and other resources.

Echo 360 (formerly known as iLecture)

Digital recordings of lectures are available. Read these instructions for details.

Technology Used

Python and GP/PARI, GnuPG, VeraCrypt, Thunderbird, Gnu Privacy Guard, Enigmail, OpenSSH, PuTTY, Ophcrack.

COVID INFORMATION

For the latest information on the University’s response to COVID-19, please refer to the Coronavirus infection page on the Macquarie website: https://www.mq.edu.au/about/coronavirus-faqs. Remember to check this page regularly in case the information and requirements change during semester. If there are any changes to this unit about COVID-19, these will be communicated via iLearn.

Unit Schedule

Week	Topic
1	Introduction to Cryptography and Elementary Number Theory
2	Symmetric Cryptography

3	Hashes, Digests and Passwords
4	Encrypting Files and Filesystems
5	Introduction to Public Key Cryptography and Advanced Number Theory
6	Digital Signatures and Authentication Protocols
7	Network and Telecommunications Security
8	ElGamal Cryptosystem and Elliptic Curve Cryptography
9	Blockchain and Cryptocurrencies I
10	Blockchain and Cryptocurrencies II
11	Quantum Computing and Post-Quantum Cryptography
12	Advanced Topics in Cryptography
13	Revision and Exam Preparation

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Assessment Procedure
- Complaints Resolution Procedure for Students and Members of the Public
- Special Consideration Policy

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

The Writing Centre

The Writing Centre provides resources to develop your English language proficiency, academic writing, and communication skills.

- Workshops
- Chat with a WriteWISE peer writing leader
- Access StudyWISE
- Upload an assignment to Studiosity
- Complete the Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and

processes

Student Enquiries

Got a question? Ask us via AskMQ, or contact Service Connect.

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Changes from Previous Offering

We value student feedback to be able to continually improve the way we offer our units. As such we encourage students to provide constructive feedback via student surveys, to the teaching staff directly, or via the FSE Student Experience & Feedback link in the iLearn page.

Unit information based on version 2024.02 of the Handbook