



COMP6300

Applied Cryptography

Session 2, In person-scheduled-weekday, North Ryde 2026

School of Computing

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	3
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	5
<u>Delivery and Resources</u>	6
<u>Unit Schedule</u>	7
<u>Policies and Procedures</u>	8
<u>Changes from Previous Offering</u>	10

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

Unit Convenor & Lecturer

Xuyun Zhang

xuyun.zhang@mq.edu.au

Contact via 98508229

Room 287, 4 Research Park Drive

Contact via Email

Lecturer

Hassan Asghar

hassan.asghar@mq.edu.au

Contact via 98509521

Room 210, 4 Research Park Drive

Contact via Email

Credit points

10

Prerequisites

Corequisites

Co-badged status

Co-badged with COMP2300

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.

Learning in this unit enhances student understanding of global challenges identified by the United Nations Sustainable Development Goals ([UNSDGs](#)) Industry, Innovation and Infrastructure

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

Requirements to Pass this Unit

To pass this unit, you must:

- Achieve a total mark equal to or greater than 50%

Assessments where Late Submissions will be accepted

- Projects 1 and 2 – YES, Standard Late Penalty applies
- Final Exam - NO, unless Special Consideration is Granted

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/assessments-exams/assessments> for more information.

- The submission time for all uploaded assessments is **11:55 pm**. A 1-hour grace period will be provided to students who experience technical concerns.
- **5% penalty per day:** If you submit your assessment late, **5% of the total possible marks** will be deducted for each day (including weekends), up to 7 days.
 - *Example 1 (out of 100):* If you score 85/100 but submit 20 hours late, you will lose 5 marks and receive **80/100**.
 - *Example 2 (out of 30):* If you score 27/30 but submit 1 day late, you will lose 1.5 marks and receive **25.5/30**.
- **After 7 days:** Submissions more than 7 days late will receive a **mark of 0**.
- **Extensions:**
 - **Automatic short extension:** Some assessments are eligible for automatic short extension. You can only apply for an automatic short extension before the due

date.

- **Special Consideration:** If you need more time due to serious issues and for any assessments that are not eligible for Short Extension, you must apply for Special Consideration.

Need help? Review the Special Consideration page [HERE](#)

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 Exams* If you experience circumstances or events that affect your ability to complete the projects and final exam in this unit on time, please inform the convenor and submit a Special Consideration request through <http://connect.mq.edu.au/>.

Project Release Dates

- Project 1: To be released no later than Friday Week 2 (07/08/2026).
- Project 2: To be released no later than Friday Week 7 (11/09/2026).

AI Approach

A recent study found that outsourcing thinking to external tools like AI can weaken our brain's memory systems, hindering critical thinking and skill development ([Oakley et al., 2025](#)). It is therefore important to help students develop productive habits of AI use, drawing on its strengths to extend, rather than replace, their own development.

The university has taken a 'two lane' approach with GenAI: assessments can be AI Open and Observed.

- AI Open: These assessments do not restrict the application of AI tools. However, it is expected that the use of AI is acknowledged in an appropriate manner, similarly to an expectation to provide references for other resources or tools that are used in producing your work.
- AI Observed: These tasks are either fully or partly observed or invigilated. AI use will either not be permitted or might be restricted in a particular way during the assessment.

Please refer to the [Assessment and AI web page](#) for information about the two-lane approach.

Please refer to the [Responsible and Ethical Use of Artificial Intelligence](#) policy page.

Assessment Tasks

Name	Weighting	Hurdle	Due	Groupwork/Individual	Short Extension	AI Approach
Exam	40%	No	Exam Period	Individual	No	Observed
Implementation of Cryptosystems	30%	No	06/09/2026	Individual	Yes	Open
Fundamentals of Cryptosystems	30%	No	25/10/2026	Individual	Yes	Open

Exam

Assessment Type ¹: Examination

Indicative Time on Task ²: 30 hours

Due: **Exam Period**

Weighting: **40%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Observed

This exam will test your understanding of material covered across the entire unit.

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.

Implementation of Cryptosystems

Assessment Type ¹: Experiential task

Indicative Time on Task ²: 20 hours

Due: **06/09/2026**

Weighting: **30%**

Groupwork/Individual: Individual

Short extension ³: Yes

AI Approach: Open

This project deals with programming for symmetric-key and public-key cryptography. You will complete the tasks of filling in missing details and correcting errors in the implementation of cryptographic algorithms in the Python programming language with a cryptographic library.

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

Fundamentals of Cryptosystems

Assessment Type ¹: Experiential task

Indicative Time on Task ²: 20 hours

Due: **25/10/2026**

Weighting: **30%**

Groupwork/Individual: Individual

Short extension ³: Yes

AI Approach: Open

This project deals with mathematics behind cryptography and elementary symmetric key cryptography. You will be required to complete mathematical analysis of discrete structures including groups and fields that are used in cryptosystems, analysis of historic ciphers and simple symmetric key cryptography algorithms.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Decipher simple encrypted messages using a range of cryptanalysis methods.

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
- [Academic Success](#) 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.

³ An automatic short extension is available for some assessments. Apply through the [Service Connect Portal](#).

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**.

You should have selected a practical at enrollment.

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 Convener](#) 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.

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 in Echo 360 which you can find in iLearn.

Technology Used

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

Unit Schedule

Week	Topic
1	Introduction to Cryptography

2	Symmetric Cryptography
3	Encrypting Files and Filesystems
4	Hashes and Digests
5	Public Key Cryptography
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) (<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) (<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) (<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 connect.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/>

Academic Success

[Academic Success](#) provides resources to develop your English language proficiency, academic writing, and communication skills.

- [Ask a Study Coach](#)
- [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 the [Service Connect Portal](#), or contact [Service Connect](#).

IT Help

For help with University computer systems and technology, visit <https://students.mq.edu.au/support/technology/service-desk>.

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.

Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff. As such, no change to the delivery of the unit is planned, however we will continue to strive to improve the level of support and the level of student engagement.

Unit information based on version 2026.04 of the [Handbook](#)