



ITEC643

Cryptography and Information Security

S2 Day 2019

Dept of Computing

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	3
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	3
<u>Delivery and Resources</u>	6
<u>Unit Schedule</u>	7
<u>Learning and Teaching Activities</u>	8
<u>Policies and Procedures</u>	8
<u>Graduate Capabilities</u>	10
<u>Changes from Previous Offering</u>	15
<u>Grading Standards</u>	15
<u>Changes since First Published</u>	17

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

Christophe Doche

christophe.doche@mq.edu.au

Contact via By email

BD building Level 2

TBA

Lecturer

Les Bell

les.bell@mq.edu.au

TBA

Lecturer

Alireza Jolfaei

alireza.jolfaei@mq.edu.au

BD Building Level 3

Tutor

Mohamadali Mehrabi

mohamadali.mehrabi@mq.edu.au

BD Building Level 2

Credit points

4

Prerequisites

Admission to MInfoTech or MEng or MSc or MScInnovation or GradDipIT or MInfoTech(Cyber Sec)

Corequisites

Co-badged status

COMP343 / ITEC643

Unit description

This unit provides an introduction to modern cryptography and information security. First, some cryptographic primitives, such as private key and public key ciphers, hash functions and digital signatures, are introduced. Then, some security technologies are discussed to illustrate how basic cryptographic primitives are concretely used in real life applications. Various attacks on the cryptographic schemes and protocols are also discussed.

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:

- 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

General Assessment Information

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Supplementary Exam

If you receive Special Consideration for the final exam, a supplementary exam will be scheduled after the normal exam period, following the release of marks. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. Approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

Assessment Tasks

Name	Weighting	Hurdle	Due
Tutorial Tasks	10%	Yes	Weekly
Assignment 1	15%	No	Week 7
Assignment 2	15%	No	Week 12
Module Exam #1	20%	No	Week 5

Name	Weighting	Hurdle	Due
Module Exam #2	20%	No	Week 9
Module Exam #3	20%	No	Week 13

Tutorial Tasks

Due: **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

Assignment 1

Due: **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

Assignment 2

Due: **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 #1

Due: **Week 5**

Weighting: **20%**

A 50 minutes long written examination worth 15% 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

Module Exam #2

Due: **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
- 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 #3

Due: **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:

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

Delivery and Resources

COMPUTING FACILITIES

Important! Please note that ITEC643 is a BYOD (Bring Your Own Device) unit since 2016. 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 three hours of lectures and a one-hour workshop every week. There uses 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 **Workshops commence in week 1**.

You should have selected a practical at enrollment.

Please note that you will be **required** to submit work every week. Failure to do so may result in you failing the unit or being excluded from the exam.

DISCUSSION BOARDS

This unit makes use of discussion boards hosted within iLearn . Please post questions there; they are monitored by the staff on the unit.

REQUIRED AND RECOMMENDED TEXTS AND/OR MATERIALS

Required readings for this unit:

- Cryptography Engineering: Design Principles and Practical Applications, Ferguson, Neils, Tadayoshi Kohno and Bruce Schneier, 1st ed., Wiley
- R. Anderson, [Security Engineering \(SE\)](#) Wiley Publishing, Inc. 2008. The complete second edition is now available online at <http://www.cl.cam.ac.uk/~rja14/book.html>

Recommended readings for this unit:

- A. J. Menezes, P. C. van Oorschot 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/>

- **NIST SP 800** documents available from <http://csrc.nist.gov/publications/PubsSPs.html>
- **IETF RFC's** available from <http://www.rfc-editor.org>
- Bauer, Craig P., **Secret History: The Story of Cryptology**, CRC Press (2013)
- N. Smart, **Cryptography: An introduction**, McGraw-Hill. The 3rd edition is available online at http://www.cs.bris.ac.uk/~nigel/Crypto_Book/

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

Java or C++ programming language and GP/PARI, GnuPG, VeraCrypt, Thunderbird, Gnu Privacy Guard, Enigmail, OpenSSH, PuTTY, Ophcrack.

Unit Schedule

Week	Topic	Reading
1	Introduction to Cryptography and elementary Number Theory	Lecture Slides
2	Modern Symmetric Ciphers	Lecture Slides
3	Cryptographic Hash Functions and Constructions	
4	Cryptanalysis and Attack Models	Lecture Slides
5	Advanced Number Theory and Introduction to public-key cryptography	Lecture Slides
6	RSA Cryptosystem	
7	ElGamal Cryptosystem and Elliptic Curve Cryptography	
8	Digital Signatures	Lecture Slides
9	Protocols I	Lecture Slides

10	Protocols II	Lecture Slides
11	Applications	Lecture Slides
12	The Frontier	Lecture Slides
13	Revision and exam preparation	

Learning and Teaching Activities

Lectures

The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.

Workshops

The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central \(https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central\)](https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). 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](#)
- [Grade Appeal Policy](#)
- [Complaint Management Procedure for Students and Members of the Public](#)
- [Special Consideration Policy](#) (**Note:** *The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.*)

Undergraduate students seeking more policy resources can visit the [Student Policy Gateway \(https://students.mq.edu.au/support/study/student-policy-gateway\)](https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the

key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit [Policy Central \(http://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central\)](http://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: <https://students.mq.edu.au/study/getting-started/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

Student Support

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

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to improve your marks and take control of your study.

- [Workshops](#)
- [StudyWise](#)
- [Academic Integrity Module for Students](#)
- [Ask a Learning Adviser](#)

Student Services and Support

Students with a disability are encouraged to contact the [Disability Service](#) who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

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.

Graduate Capabilities

Creative and Innovative

Our graduates will also be capable of creative thinking and of creating knowledge. They will be imaginative and open to experience and capable of innovation at work and in the community. We want them to be engaged in applying their critical, creative thinking.

This graduate capability is supported by:

Learning outcomes

- 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

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Module Exam #1
- Module Exam #2
- Module Exam #3

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.
- The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Capable of Professional and Personal Judgement and Initiative

We want our graduates to have emotional intelligence and sound interpersonal skills and to demonstrate discernment and common sense in their professional and personal judgement. They will exercise initiative as needed. They will be capable of risk assessment, and be able to handle ambiguity and complexity, enabling them to be adaptable in diverse and changing environments.

This graduate capability is supported by:

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.
- The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Discipline Specific Knowledge and Skills

Our graduates will take with them the intellectual development, depth and breadth of knowledge, scholarly understanding, and specific subject content in their chosen fields to make them competent and confident in their subject or profession. They will be able to demonstrate, where relevant, professional technical competence and meet professional standards. They will be able to articulate the structure of knowledge of their discipline, be able to adapt discipline-specific knowledge to novel situations, and be able to contribute from their discipline to inter-disciplinary solutions to problems.

This graduate capability is supported by:

Learning outcomes

- 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

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Module Exam #1
- Module Exam #2
- Module Exam #3

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.
- The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Critical, Analytical and Integrative Thinking

We want our graduates to be capable of reasoning, questioning and analysing, and to integrate and synthesise learning and knowledge from a range of sources and environments; to be able to critique constraints, assumptions and limitations; to be able to think independently and systemically in relation to scholarly activity, in the workplace, and in the world. We want them to have a level of scientific and information technology literacy.

This graduate capability is supported by:

Learning outcomes

- 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

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Module Exam #1
- Module Exam #2
- Module Exam #3

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.

Problem Solving and Research Capability

Our graduates should be capable of researching; of analysing, and interpreting and assessing data and information in various forms; of drawing connections across fields of knowledge; and they should be able to relate their knowledge to complex situations at work or in the world, in order to diagnose and solve problems. We want them to have the confidence to take the initiative in doing so, within an awareness of their own limitations.

This graduate capability is supported by:

Learning outcomes

- 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

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Module Exam #1
- Module Exam #2
- Module Exam #3

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.
- The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Effective Communication

We want to develop in our students the ability to communicate and convey their views in forms effective with different audiences. We want our graduates to take with them the capability to read, listen, question, gather and evaluate information resources in a variety of formats, assess, write clearly, speak effectively, and to use visual communication and communication technologies as appropriate.

This graduate capability is supported by:

Learning outcomes

- Decipher simple encrypted messages using a range of cryptanalysis methods
- Apply cryptographic technologies and protocols to increase data security and protect privacy

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Module Exam #1
- Module Exam #2
- Module Exam #3

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.

- The practicals provide opportunities for hands-on learning in three primary areas: low-level programming skills, the number theory which underlies public-key cryptography and the practical application of security technologies such as file and disk encryption as well as the exchange of signed and encrypted emails. Important! Please note that ITEC643 will be a BYOD (Bring Your Own Device) unit in 2019. You will be expected to bring your own laptop computer (Windows, Mac or Linux) to the Tutorial/Practicals, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Engaged and Ethical Local and Global citizens

As local citizens our graduates will be aware of indigenous perspectives and of the nation's historical context. They will be engaged with the challenges of contemporary society and with knowledge and ideas. We want our graduates to have respect for diversity, to be open-minded, sensitive to others and inclusive, and to be open to other cultures and perspectives: they should have a level of cultural literacy. Our graduates should be aware of disadvantage and social justice, and be willing to participate to help create a wiser and better society.

This graduate capability is supported by:

Learning and teaching activities

- The lectures are the primary activity for this unit. While the lecture notes or slides will be available on iLearn, a lot of supporting detail and explanation is presented in the lectures, so skipping them is inadvisable.

Changes from Previous Offering

- In the past, ITEC643 was dealing with cryptography and information security. From 2019, Session 2, ITEC643 exclusively focuses on applied cryptography.
- The unit has been organised around three distinct modules. Symmetric-key Cryptography from week 1 to 4, then Public-key cryptography from week 5 to 8 and finally Protocols and Applications from week 9 to 12.
- There is no mid-term test nor final examination as each part is now assessed via a module examination worth 20%. Module exams are not a hurdle.

Grading Standards

At the end of the semester, you will receive a grade that reflects your achievement in the unit

- **Fail (F):** does not provide evidence of attainment of all learning outcomes. There is missing or partial or superficial or faulty understanding and application of the

fundamental concepts in the field of study; and incomplete, confusing or lacking communication of ideas in ways that give little attention to the conventions of the discipline.

- **Pass (P):** provides sufficient evidence of the achievement of learning outcomes. There is demonstration of understanding and application of fundamental concepts of the field of study; and communication of information and ideas adequately in terms of the conventions of the discipline. The learning attainment is considered satisfactory or adequate or competent or capable in relation to the specified outcomes.
- **Credit (Cr):** provides evidence of learning that goes beyond replication of content knowledge or skills relevant to the learning outcomes. There is demonstration of substantial understanding of fundamental concepts in the field of study and the ability to apply these concepts in a variety of contexts; plus communication of ideas fluently and clearly in terms of the conventions of the discipline.
- **Distinction (D):** provides evidence of integration and evaluation of critical ideas, principles and theories, distinctive insight and ability in applying relevant skills and concepts in relation to learning outcomes. There is demonstration of frequent originality in defining and analysing issues or problems and providing solutions; and the use of means of communication appropriate to the discipline and the audience.
- **High Distinction (HD):** provides consistent evidence of deep and critical understanding in relation to the learning outcomes. There is substantial originality and insight in identifying, generating and communicating competing arguments, perspectives or problem solving approaches; critical evaluation of problems, their solutions and their implications; creativity in application.

Your final grade depends on your performance in each assessment task and on your ability to perform well enough on the hurdle assessment tasks.

For each task, you receive a mark that reflects your standard of performance. Then the different component marks are added up to determine an aggregated mark out of 100. In order to pass the unit, this aggregated mark needs to be at least 50.

You also need to be achieve a minimum standard of performance on the hurdle assessment tasks.

Hurdle Assessment Task

- Submission of tutorial tasks in this unit is a hurdle requirement. You are required to make at least 8 out of 12 submissions in order to pass the unit.

Not that assignment submission in this unit is not a hurdle requirement. However, if you do not make a reasonable attempt at the two assignments, you will be unlikely to pass the unit.

Your final grade is then a direct reflection of the aggregated mark (provided that you satisfy the hurdle requirements) according to the following:

- 85-100 for **HD**
- 75-84 for **D**
- 65-74 for **CR**
- 50-64 for **P**

If you receive special consideration for the final exam, a supplementary exam will be scheduled in the interval between the regular exam period and the start of the next session. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. You can check the supplementary exam information page on FSE101 in iLearn (bit.ly/FSESupp) for dates, and approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

If you are given a second opportunity to sit the final examination as a result of failing to meet the minimum mark required, you will be offered that chance during the same supplementary examination period and will be notified of the exact day and time after the publication of final results for the unit.

Changes since First Published

Date	Description
25/07/2019	Made a few cosmetic changes. Added a tutor, changes assignment submissions deadline and fixed typos