# ITEC643

## Cryptography and Information Security

S1 Day 2017

*Dept of Computing*

## Contents


General Information 2

Learning Outcomes 3

Assessment Tasks 3

Delivery and Resources 6

Unit Schedule 7

Learning and Teaching Activities 8

Policies and Procedures 9

Graduate Capabilities 10

Changes from Previous Offering 17

Grading Standards 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, lecturer
Christophe Doche
christophe.doche@mq.edu.au
Contact via By email
E6A371
TBA

Lecturer
Les Bell
les.bell@mq.edu.au
Available for the hour after Thursday lectures; other times by appointment.

Workshops Supervisor
Daniel Sutantyo
daniel.sutantyo@mq.edu.au
TBA

Credit points
4

Prerequisites
Admission to MInfoTech or MEng or MSc

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:

Demonstrate an understanding of the principles and concepts of cryptography and information security

Apply existing security technologies to preserve security properties of information

Apply security principles in the development of applications and systems

Relate information security to enterprise requirements and activities

# Assessment Tasks

| Name | Weighting | Hurdle | Due |
|---|---|---|---|
| Tutorial Tasks | 8% | Yes | Weekly |
| Assignment 1 | 13% | No | Week 7 |
| Assignment 2 | 13% | No | Week 12 |
| Assignment 3 | 15% | No | Week 13 |
| Mid Semester Test | 13% | No | Week 7 |
| Final Examination | 38% | Yes | TBA |

## Tutorial Tasks

Due: **Weekly**
Weighting: **8%**
**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:

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

## Assignment 1

Due: **Week 7**
Weighting: **13%**

Assignment comprises two parts. The first part involves the implementation of a hash function. The second part deals with a public key cryptoprimitives. The first part is due in week 4 and the second part is due in week 7. The assignment is to be submitted via iLearn. Late submissions attract no marks.

On successful completion you will be able to:

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply security principles in the development of applications and systems

## Assignment 2

Due: **Week 12**
Weighting: **13%**

Security Evaluation of a System or Product. The assignment is to be submitted via iLearn. Late submissions attract no marks.

On successful completion you will be able to:

- Apply existing security technologies to preserve security properties of information
- Relate information security to enterprise requirements and activities

## Assignment 3

Due: **Week 13**
Weighting: **15%**

Pick two conference talks or papers, one from a list of academic conferences and one from a list of industry conferences. Summarize and review each paper. Each summary and review should be 1200 - 1500 words long. Finally, add 500 - 1000 words summarizing the differences you have discovered between the two types of conferences and their submissions. The assignment is to be submitted via iLearn. Late submissions attract no marks.

This Assessment Task relates to the following Learning Outcomes:

- Some familiarity with contemporary information security research in both academia and industry, and how these differ.

On successful completion you will be able to:

- Relate information security to enterprise requirements and activities

## Mid Semester Test

Due: **Week 7**
Weighting: **13%**

A 50 minutes long written examination worth 15% that will be held in week 7 during class time. This will test your understanding of material covered in weeks 1 to 6. The mid-semester test has the same structure as the final examination. The feedback received will allow you to be better prepared for the final examination.

On successful completion you will be able to:

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply security principles in the development of applications and systems

## Final Examination

Due: **TBA**
Weighting: **38%**
**This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)**

The final examination is designed to test your understanding of basic concepts of modern Cryptography and Information Security. Regarding the examination process, note that:

- you must attend all required classes and submit all required assessments, otherwise the Executive Dean of the Faculty or delegated authority has the power to refuse permission to attend the final examination
- the University Examination period for Mid-Year 2017 is from Tuesday 13th June to Mon 26th June 2017
- you are expected to present yourself for examination at the time and place designated in the University Examination Timetable
- the timetable will be available in Draft form approximately eight weeks before the commencement of the examinations and in Final form approximately four weeks before the commencement of examinations
- no early examinations for individuals or groups of students will be set. All students are expected to ensure that they are available until the end of the teaching semester, that is the final day of the official examination period
- the only exception to not sitting an examination at the designated time is because of documented illness or unavoidable disruption. In these circumstances you may wish to notify the university of your circumstances, as detailed in the Disruption to Studies

Policy.

On successful completion you will be able to:

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

# Delivery and Resources

## COMPUTING FACILITIES

**Important!** Please note that COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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.

## 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 on Monday afternoons, and a third hour on Thursdays at lunch time.

There are two practical workshops, on Mondays and Thursdays, which use hands-on exercises to introduce and reinforce concepts related to the lecture content; 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 **Practicals 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:

- A. J. Menezes, P. C. van Oorrschot and S. A. Vanstone, **Handbook of applied cryptogr**

**aphy (HAC)**, CRC Press, Boca Raton, FL, 1996. All required chapters are available online at http://cacr.uwaterloo.ca/hac/

- 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:

- **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, information theory, classical ciphers up to Enigma | Lecture Slides, HAC Chapter 1.1, 2.1-2.3 |
| 2 | Introduction to elementary Number Theory - Secret-Key (Symmetric) Cryptography - Block ciphers, Stream Ciphers, Sources of Randomness | Lecture Slides, HAC 2. 6, 5.1 |
| 3 | DES and AES in detail, attacks on block ciphers | Lecture Slides, HAC 7.3, 7.4, 2.4 - 2.6 |
| 4 | Cryptographic Hash Functions and Constructions | Lecture Slides, HAC 9 |
| 5 | Public Key Cryptography - RSA, DSA, El Gamal, Attacks on RSA. | Lecture Slides, HAC 8, 11 |

| | | |
|---|---|---|
| 6 | Advanced Topics - Secret Sharing, Elliptic Curve Cryptography, Quantum Cryptography, Post-Quantum Cryptography | Lecture Slides |
| 7 | Introduction to infosec, encrypted files and filesystems, block cipher modes - Mid-Term Text | Lecture Slides, Verizon Data Breach Investigation Report |
| 8 | Encrypted files and filesystems, block cipher modes | Lecture Notes |
| 9 | Authentication, protocols, signatures | Lecture Slides, SE Chapters 3, 5, 15 |
| 10 | Encryption for network communications - SSL, SSH, PGP | Lecture Slides, Notes, SE Chapter 20 |
| 11 | Access control - discretionary access control in UNIX and Windows, mandatory access control and trusted systems, security models for applications | Lecture Slides, Notes, SE Chapters 4, 8, 9 |
| 12 | Software security, security assessment and penetration testing, incident response and forensics | Lecture Slides, Notes , SE Chapter 25 |
| 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.

## Tutorials

The tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.

## Practicals

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 COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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.

## Readings

Two required textbooks have been selected - both can be downloaded at no cost in PDF format.

The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

# Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central. Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

Assessment Policy http://mq.edu.au/policy/docs/assessment/policy_2016.html

Grade Appeal Policy http://mq.edu.au/policy/docs/gradeappeal/policy.html

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy (in effect until Dec 4th, 2017): http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

Special Consideration Policy (in effect from Dec 4th, 2017): https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration

In addition, a number of other policies can be found in the Learning and Teaching Category of 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/support/student_conduct/

## Results

Results shown in *iLearn*, 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.

# 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

## 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

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

### Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Assignment 3
- Mid Semester Test
- Final Examination

### 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 tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.
- 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 COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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.
- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

## 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 COMP343

will be a BYOD (Bring Your Own Device) unit in 2016. 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.

- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

## Commitment to Continuous Learning

Our graduates will have enquiring minds and a literate curiosity which will lead them to pursue knowledge for its own sake. They will continue to pursue learning in their careers and as they participate in the world. They will be capable of reflecting on their experiences and relationships with others and the environment, learning from them, and growing - personally, professionally and socially.

This graduate capability is supported by:

### Learning and teaching activities

- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

## 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

- Demonstrate an understanding of the principles and concepts of cryptography and

information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

## Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Mid Semester Test
- Final Examination

## 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 tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.
- 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 COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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.
- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

# 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

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

## Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Assignment 3
- Mid Semester Test
- Final Examination

## 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 tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.
- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

# 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

- Demonstrate an understanding of the principles and concepts of cryptography and information security
- Apply existing security technologies to preserve security properties of information
- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

## Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Mid Semester Test
- Final Examination

## 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 tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.
- 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 COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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.
- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings

and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

## 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

- Apply security principles in the development of applications and systems
- Relate information security to enterprise requirements and activities

### Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Assignment 3
- Mid Semester Test
- Final Examination

### 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 tutorials are workshop-style interactive sessions which relate the theory from the lectures to the practical sessions which follow. The tutorials also provide material which may fill in gaps in students' knowledge and establish some basic skills which will be useful in the practicals and Assignment 1.
- 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 COMP343 will be a BYOD (Bring Your Own Device) unit in 2016. 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:

### Assessment task

- Assignment 3

### Learning and teaching activity

- 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.
- Two required textbooks have been selected - both can be downloaded at no cost in PDF format. The Handbook of Applied Cryptography covers the mathematical underpinnings and details of modern cryptographic techniques, and will be used throughout the first half of the unit. Security Engineering deals with information security principles in general and the practical implementation of cryptosystems, and will be used throughout the second half of the unit.

# Changes from Previous Offering

- While in previous years, students were *encouraged* to complete the practicals on their own computer, in 2017 this will become *standard practice*. Students will be expected to install the required software and complete practicals and tutorial exercises on their own computers.
- Tutorial tasks and final examination are now hurdle assessment tasks. See next section on grading to fully understand what that means.

# 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 Tasks**

- 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.

- The final examination in this unit is a hurdle requirement. You must get a mark of at least 40 out of 100 in the final examination to clear the hurdle and pass the unit. If you get a mark of at least 30 out of 100 in the final examination, but fail to pass the unit overall, you will be given a second and final attempt to resit and pass the final examination.

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 apply for Disruption to Study for your final examination, you must make yourself available for the week of July 24 – 28, 2017. If you are not available at that time, there is no guarantee an additional examination time will be offered. Specific examination dates and times will be determined at a later date.

Second-chance hurdle examinations will also be offered in the week of July 24 - 28. Results will be released on July 13. You will be notified shortly after that date of your eligibility for a hurdle retry and you must also make yourself available during that week to take advantage of this opportunity.