COMP343

Cryptography and Information Security

S1 Day 2014

Computing

Contents

General Information

Unit convenor and teaching staff
Other Staff
Leslie Bell
les.bell@mq.edu.au
Contact via les.bell@mq.edu.au
E6A 354
one hour after each lecture plus other times by appointment

Unit Convenor
Christophe Doche
christophe.doche@mq.edu.au
Contact via christophe.doche@mq.edu.au

Credit points
3

Prerequisites
39cp and (COMP125(P) or COMP165(P)) and (DMTH137(P) or MATH237(P) or DMTH237(P))

Corequisites

Co-badged status

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 basic concepts of modern cryptography and the elementary principles of information security

Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication

Implement cryptographic algorithms and protocols using java

Assessment Tasks

Name	Weighting	Due
Tutorial Tasks	10%	Weekly
Assignment 1	15%	Week 7
Assignment 2	15%	Week 12
Mid-semester test	15%	Week 6
Final exam	45%	TBA

Tutorial Tasks

Due: **Weekly**
Weighting: **10%**

Each week, a set of exercises will be available online. The first of the tutorial exercises for the week is the task you need to solve. 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 basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication
- Implement cryptographic algorithms and protocols using java

Assignment 1

Due: **Week 7**
Weighting: **15%**

Implementation of a cipher. 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 basic concepts of modern cryptography and the elementary principles of information security

- Implement cryptographic algorithms and protocols using java

Assignment 2

Due: **Week 12**
Weighting: **15%**

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:

- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication

Mid-semester test

Due: **Week 6**
Weighting: **15%**

It is a 50 minutes long written examination worth 15% that will be held in week 6 during class time. It will test your understanding of material covered in weeks 1 to 5. 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 basic concepts of modern cryptography and the elementary principles of information security

Final exam

Due: **TBA**
Weighting: **45%**

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 assessment, 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 2014 is from Monday 16th June to Friday 4th July 2014
- 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 consider applying for Special Consideration.

On successful completion you will be able to:

- Demonstrate an understanding of the basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication

Delivery and Resources

CLASSES

Each week you should read the slides and prepare for the lectures. The first hour of lecture every Tuesday is especially important as it is delivered in a more interactive tutorial style. The next two hours of lectures are on Wednesday. There is also a one hour practical. 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 enrolment.

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.

REQUIRED AND RECOMMENDED TEXTS AND/OR MATERIALS

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. Sample chapters 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
- **NIST SP 800** documents available from http://csrc.nist.gov/publications/PubsSPs.html
- **IETF RFC's** available from http://www.rfc-editor.org

- 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,...

Echo 360 (formerly known as iLecture)

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

Technology Used

Java programming language and PARI, GnuPG, TrueCrypt, Thunderbird, OpenSSH, PuTTY

Unit Schedule

1	Introduction to cryptography	Lecture slides Week 1
2, 3	Symmetric Key Cryptography	Lecture slides Week 2, 3
4	Cryptographic Hashing	Lecture slides Week 4
5	Public Key Cryptography	Lecture slides Week 5
6	Public Key Cryptography + Mid-Term Test	Lecture slides Week 5
7	Encrypted files and file systems (data at rest)	Lecture slides + SE Chap. 5 + NIST SP 800-38a, IEEE Std 1619-2007, SP 800-38E
8	Symmetric encryption for data in motion	Lecture slides + SE Chap. 21 (1st ed.: 18), NIST SP800-38a, RFC 4346 (TLS 1.1) + RFC 5246 (TLS 1.2), notes on SSH
9	Authentication	Lecture slides + SE Chaps. 3 and 15
10	Access control	Lecture slides + SE Chaps. 4, 8, 9, notes on UNIX permissions
11	eMoney, eVoting, Digital Rights Management	Lecture slides + SE Chaps. 10, 22
12	Revision	Lecture slides
13	Revision	Lecture slides

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.html

Grading Policy http://mq.edu.au/policy/docs/grading/policy.html

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

Grievance Management Policy http://mq.edu.au/policy/docs/grievance_management/policy.html

Disruption to Studies Policy http://www.mq.edu.au/policy/docs/disruption_studies/policy.html *The Disruption to Studies Policy is effective from March 3 2014 and replaces the Special Consideration Policy.*

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/

Departmental Special Consideration Policy http://comp.mq.edu.au/undergrad/policies/special_consideration_policy.htm

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://informatics.mq.edu.au/help/.

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

Graduate Capabilities

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 basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication
- Implement cryptographic algorithms and protocols using java

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Mid-semester test
- Final exam

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 basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication
- Implement cryptographic algorithms and protocols using java

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Mid-semester test
- Final exam

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 basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication
- Implement cryptographic algorithms and protocols using java

Assessment tasks

- Tutorial Tasks
- Assignment 1
- Assignment 2
- Mid-semester test
- Final exam

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 basic concepts of modern cryptography and the elementary principles of information security
- Use security technologies effectively in order to achieve elementary information security goals, such as integrity, confidentiality, and authentication
- Implement cryptographic algorithms and protocols using java

Assessment task

- Tutorial Tasks

Grading Standards

Four standards, namely Developing, Functional, Proficient, and Advanced, summarize as many different levels of achievement. Each standard is precisely defined to help students know what kind of performance is expected to deserve a certain mark. The standards corresponding to the learning outcomes of this unit are given below:

Learning Outcome #1	Developing	Functional	Proficient	Advanced
	Understand some concepts of symmetric-key and public-key encryption and cryptographic hashing. Close to a correct formulation of some cryptographic attacks.	Understand basic concepts of symmetric-key and public-key encryption and cryptographic hashing. Correct formulation of basic cryptographic attacks.	Understand concepts of symmetric-key and public-key encryption and cryptographic hashing in details. Ability to describe basic cryptographic attacks in details with the understanding the relation between the security parameters and the complexity of cryptanalysis.	Master concepts of symmetric-key and public-key encryption and cryptographic hashing. Ability to describe all cryptographic attacks covered at lectures and tutorials in detail with an understanding of the relation between the security parameters and the complexity of cryptanalysis.
Learning Outcome #2				

	Limited understanding of the fundamental concepts of information security. Some ability to apply basic cryptographic and security tools to achieve the required security goal. Limited ability to analyse security level achived.	Understanding of the concepts of information security. Ability to apply basic cryptographic and security tools to achieve the required security goals. Ability to analyse the security level achieved.	Understanding of the concepts of information security and their relations. Ability to apply basic cryptographic and security tools to achieve the required security goals. Ability to analyse the security level achieved supported by evidence.	Deep Understanding of the concepts of information security, their relationsand limitations. Ability to apply basic cryptographic and security tools to achieve the required security goals. Ability to analyse the security level achieved supported by theoretical arguments.
Learning Outcome #3				
	Limited ability to implement a correct java program following specifications	Correctly implement low-level bit-manipulation mechanisms of a cryptoprimitve in Java; implement a Java program following specifications	Write efficient, well-documented Java code which implements a cryptoprimitve in Java and utilise this in a Java program which meets specifications	Design well-architected, efficient and well-documented Java program code to implement a cryptoprimitve, together with all required tests and demonstration program, following good design and test practice

Grading

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.

The relation between standards and grades can be loosely described as follows. If you consistently fail to reach any standard, you will fail the unit. If you consistently achieve

- Functional standards, you will get a P grade.
- Proficient standards, you will get a Cr/D grade.
- Advanced standards, you will get an HD grade.

More precisely, your final grade depends on your performance in each part of the assessment. For each task, you receive a mark that combines your standard of performance regarding each learning outcome assessed by this task. Then the different component marks are added up to determine your total mark out of 100. Your grade then depends on this total mark and your overall standards of performance.

In particular, **in order to pass the unit**, you must

- Total mark -- have a total mark of 50 or above; and
- Pass the combined mid semester test and final, i.e. obtain more than 30% out of 60% for those two assessment tasks

In order to obtain a higher grade than a Pass, you must fulfill the pass requirements and get an overall total mark in the range:

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

What has changed since last offering

Programming Language

We use java for all implementation tasks as opposed to C++ last year

No lectures on Mon 9th June

Mon 9th June is a public holiday. No class will be held on that day.