AMSI Online: Honours and Masters Subject Guide

Frontiers of Applied Cryptography

Semester 2, 2026

Administration and contact details

Host department	School of Science, Discipline of Mathematics
Host institution	RMIT University
Name of lecturer	Dr. Arathi Arakala and Dr. Amy Corman
Phone number	99252279 and 99256482
Email address	Arathi.arakala@rmit.edu.au and amy.corman@rmit.edu.au
Homepage	https://www.rmit.edu.au/contact/staff-contacts/academic-staff/a/arakala-dr-arathi and https://www.rmit.edu.au/contact/staff-contacts/academic-staff/c/corman-dr-amy
Name of honours coordinator	Assoc. Prof. Stephen Davis
Phone number	99252278
Email address	Stephen.davis@rmit.edu.au
Name of masters coordinator	N/A
Phone number	N/A
Email address	N/A

Subject details

Handbook entry URL	
Subject homepage URL	
Honours student hand-out URL	
Teaching period (start and end date):	20 July - 18 Nov (orientation week: 13-17 July)
Exam period (start and end date):	Oct 19 to 15 Nov
Contact hours per week:	3
AMSI Online enrolment close date:	13 July
Lecture day(s) and time(s):	Tuesdays 5:30 pm to 8:30 pm
Description of electronic access arrangements for students (for example, LMS)	Teams link to access classes. LMS access will be attempted. If there are any access issues course material will be provided using email.

Subject content

1. Subject content description

The course will present technical aspects of symmetric key and public key cryptosystems and attacks on their security, as well as the algorithms for factoring and primality testing which enable the generation of public keys. The course will then focus on new developments in the field including quantum computing, quantum safe cryptography and blockchain.

2. Week-by-week topic overview

Week 1: Elliptic Curves
Week 2: Elliptic Curve Cryptography
Week 3: Linear Cryptanalysis
Week 4: Differential Cryptanalysis
Week 5: Quantum Key Distribution
Week 6: Post Quantum Cryptography
Week 7: Mid sem assessment
Week 8: Cryptographic Network Protcols
Week 9: Privacy
Week 10: Anonymity
Week 11: Blockchain algorithms
Week 12: Applications of Blockchain
Week 13: End of semester assessment
Week 14: Oral Presentations

3. Assumed prerequisite knowledge and capabilities

You should have a basic understanding of cryptography including concepts of symmetric and asymmetric ciphers. Familiarity with the R programming language is advantageous as some assessment tasks will require R

4. Learning outcomes and objectives

1. Critically review new theoretical and practical developments in cryptography and their impact on contemporary information systems.
2. Recognise and justify the role of cryptanalysis in the design of secure systems.
3. Critically analyse technical details of contemporary cryptosystems.
4. Critically evaluate technical details of potential future cryptosystems.
5. Solve cryptographic problems applying a range of theoretical and simulated practical scenarios.
6. Effectively conveying complex technical details using an array of communication methods such as written text, mathematical equations, diagrams, and innovative visualizations.
7. Justify the place of ethics in Information Security, critically reflecting on the moral imperatives of the field.

AQF specific Program Learning Outcomes and Learning Outcome Descriptors (if available):

AQF Program Learning Outcomes addressed in this subject	Associated AQF Learning Outcome Descriptors for this subject
Insert Program Learning Outcome here	Choose from list below

Learning Outcome Descriptors at AQF Level 8

Knowledge

K1: coherent and advanced knowledge of the underlying principles and concepts in one or more disciplines

K2: knowledge of research principles and methods

Skills

S1: cognitive skills to review, analyse, consolidate and synthesise knowledge to identify and provide solutions to complex problem with intellectual independence

S2: cognitive and technical skills to demonstrate a broad understanding of a body of knowledge and theoretical concepts with advanced understanding in some areas

S3: cognitive skills to exercise critical thinking and judgement in developing new understanding

S4: technical skills to design and use in a research project

S5: communication skills to present clear and coherent exposition of knowledge and ideas to a variety of audiences

Application of Knowledge and Skills

A1: with initiative and judgement in professional practice and/or scholarship

A2: to adapt knowledge and skills in diverse contexts

A3: with responsibility and accountability for own learning and practice and in collaboration with others within broad parameters

A4: to plan and execute project work and/or a piece of research and scholarship with some independence

5. Learning resources

The course reading material is provided on the course page and where appropriate video recordings of lecture topics will be provided sufficiently prior to class.

6. Assessment breakdown

- Two practical assignments due in weeks 5 and 11.
- Two timed analysis tasks in weeks 7 and 13.
- An Oral report due in Week 14 scaffolded by weekly reflections due in Weeks 2,3,4,5,6,8,9,10 and 12.
- A summary of the Oral Presentation topic is due by the end of Week 6.

Timed Analysis	**50%**
Practical Assignment	**30%**
Oral and Written Reflections	**20%**

Assignment due dates	
Practical Assignment 1	**23 Aug**
Timed analysis task 1	**8 Sep**
Practical Assignment 2	**11 Oct**
Timed Analysis Task 2	**20 Oct**
Oral Presentation	**27 Oct**

Institution honours program details

Weight of subject in total honours assessment at host department	
Thesis/subject split at host department	
Honours grade ranges at host department	
H1	Enter range %
H2a	Enter range %
H2b	Enter range %
H3	Enter range %

Institution masters program details

Weight of subject in total masters assessment at host department	
Thesis/subject split at host department	
Masters grade ranges at host department	
H1	Enter range %
H2a	Enter range %
H2b	Enter range %
H3	Enter range %