AMSI ACE NETWORK

ACE Network Subject Information Guide

Frontiers of Applied Cryptography

Semester 2, 2025

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	
Phone number	
Email address	

Subject details

Handbook entry URL	**http://www1.rmit.edu.au/browse/;CURPOS=1?STYPE=ENTIRE&CLOCATION=Study+at+RMIT%2F&QRY=%2Btype%3Dflexible+%2Bsubtype%3Dheparta+%2Bkeywords%3D%28INTE1127%29+&course=INTE1127&title=&Search=Search**
Subject homepage URL	TBD
Honours student hand-out URL	TBD
Teaching period (start and end date):	**21 July to 19 October**

Exam period (start and end date):	**20 October to 2 November**
Contact hours per week:	**1.5 hour weekly class** **1 hour weekly drop-in session (optional)**
ACE enrolment closure date:	**TBA**
Lecture day(s) and time(s):	Tuesdays from 5:30 pm to 8:30 pm.
Description of electronic access arrangements for students (for example, LMS)	**Canvas access can be given.** This will be through a Teams meeting invite. I will make the Teams link available closer to the class start

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: Block Ciphers**
- **Week 2: Elliptic Curves**
- **Week 3: Elliptic Curve Cryptography**
- **Week 4: Quantum Computing Algorithms**
- **Week 5: Post Quantum Cryptography**
- **Week 6: Quantum Key Distribution**
- **Week 7: Blockchain algorithms**
- **Week 8: Applications of Blockchain**
- **Week 9: Anonymity and Privacy**
- **Week 10: Applications of Anonymity and Privacy**
- **Week 11: Protocol Attacks**
- **Week 12: Homomorphic Encryption**

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
Insert Program Learning Outcome here	Choose from list below
Insert Program Learning Outcome here	Choose from list below
Insert Program Learning Outcome here	Choose from list below
Insert Program Learning Outcome here	Choose from list below
Insert Program Learning Outcome here	Choose from list below
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

R.L. Burden and J.D. Faires, Numerical Analysis, 9th edition, Brooks and Cole

- Brockwell, P. and Davis, R., An Introduction to Time Series and Forecasting, Springer-Verlag, 1996.

6. Assessment

Exam/assignment/classwork breakdown						
Report	20%	**Practical Assessment**	30%	**In class Asses**	50 %	
Assignment due dates		**Week 4 (Practical)**	**Week 6 (In-class test)**	Week 7 (Practical)	Week 11 (Practical)	**Week 12 (In-class test)**
Approximate exam date				**TBA**		

Institution honours program details – To Be Determined

Weight of subject in total honours assessment at host department	Click here to enter text.
Thesis/subject split at host department	Click here to enter text.

Honours grade ranges at host department	
H1	Enter range %
H2a	Enter range %
H2b	Enter range %
H3	Enter range %

Institution masters program details – To Be Determined

Weight of subject in total masters assessment at host department	Click here to enter text.
Thesis/subject split at host department	Click here to enter text.
Masters grade ranges at host department	
H1	Enter range %
H2a	Enter range %
H2b	Enter range %
H3	Enter range %