



ACE Network Subject Information Guide

Data Security

Semester 1, 2025

Administration and contact details

Host department	School of Information and Physical Sciences
Host institution	University of Newcastle
Name of lecturer	Dr. Saiful Islam
Phone number	0424422409
Email address	saiful.islam@newcastle.edu.au
Homepage	https://www.newcastle.edu.au/profile/saiful-islam
Name of honours coordinator (Bachelor of Computing - Honours)	Dr Kyle Harrison
Phone number	(02) 4055 0738
Email address	kyle.harrison@newcastle.edu.au
Name of masters coordinator (Master of Data Science and AI)	Dr. Weijia Zhang
Phone number	(02) 4055 0921
Email address	weijia.zhang@newcastle.edu.au

Subject details

Handbook entry URL	https://handbook.newcastle.edu.au/course/2025/COMP6360
Subject homepage URL	https://handbook.newcastle.edu.au/course/2025/COMP6360
Honours student hand-out URL	https://handbook.newcastle.edu.au/program/2025/40283
Teaching period (start and end date):	24 February 2025 – 6 June 2025
Exam period (start and end date):	10 June 2025 – 20 June 2025
Contact hours per week:	4
ACE enrolment closure date:	TBA
Lecture day(s) and time(s):	Monday 12:00pm to 2:00pm (Lecture ONLINE) Tuesday 12:00pm to 2:00 pm (Workshop ONLINE)
Description of electronic access arrangements for students (for example, LMS)	Access will be arranged for the relevant Canvas/Catalog page

Subject content

1. Information and number theory, finite fields
2. Classical cryptography
3. Contemporary symmetric cyphers
4. Public key cryptography
5. Key management
6. Authentication and digital signatures
7. Privacy and Privacy Enhancing Technologies
8. Advanced topics: Elliptic curve cryptography and homomorphic encryption
9. Applications: Privacy in social networks, electronic voting, digital cash

1. Week-by-week topic overview

Week 1: Introduction to Data Security, Revision: Groups, rings, fields

Week 2: Number theory,

Week 3: Information theory, perfect secrecy, unicity distance

Week 4: Classical ciphers

Week 5: Stream and block ciphers; Feistel cipher; DES and DES modes of operation

Week 6: AES; AES polynomial arithmetic

Week 7: PK Encryption, RSA, ElGamal; elliptic Curves

Week 8: Key management; message authentication

Week 9: Hash functions and digital signatures

Week 10: Selected topics in cryptography and security

Week 11: Privacy; selected topics in cryptography and security

Week 12: Privacy; selected topics in cryptography and security

Week 13: Revision

2. Assumed prerequisite knowledge and capabilities

Programming experience (Python, C/C++, Or Java)

Knowledge of discrete mathematics

3. Learning outcomes and objectives

Upon completion of this course, graduates will be able to:

1. Break classical ciphers
2. Apply number and information theories to modern cryptography
3. Analyse and evaluate modern cryptographic systems
4. Design a system that will provide encryption, decryption, signature and forward security
5. Assess security and privacy in data publishing, social networks, electric voting and digital cash

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

4. Learning resources

W. Stallings. Cryptography and Network Security, Global Edition, Pearson Education Australia, 2016.

5. Assessment

Exam/assignment/classwork breakdown					
Final Exam	40%	Assignments	40%	In Term Test and Weekly quizzes	20%
Assignment due dates		Assignment 1 Week 7	Assignment 2 Week 12	Friday 11:59 PM of Week 7	Friday 11:59 PM of Week 12
Approximate exam date					
In Term Test					Week 5 (During Lecture/ONLINE)
Final Exam					10 June 2025 – 20 June 2025

Institution honours program details – To Be Determined

Weight of subject in total honours assessment at host department	10 units of 80 total
Thesis/subject split at host department	60 units of 80 total
Honours grade ranges at host department	
H1	85 - 100%
H2a	75 – 84 %
H2b	65 – 74 %
H3	50 – 64 %

Institution masters program details – To Be Determined

Weight of subject in total masters assessment at host department	10 units of 120 total
Thesis/subject split at host department	20 units of 120 total
Masters grade ranges at host department	
HD	85 - 100%
D	75 – 84%
C	65 – 74%
P	50 – 64 %