School of Information and Physical Sciences

COMP6360: Data Security

Callaghan
Semester 1 - 2024

COURSE OUTLINE

OVERVIEW

Course Description
This course deals with topics in cryptography and data security. Students learn fundamental technical tools for cryptography and data security, as well as how to combine the tools to support various security requirements in computerised data processing, data storing and communication.

Academic Progress Requirements
Nil

Assumed Knowledge
SENG6110SENG6120 Knowledge of discrete mathematics.

Contact Hours

Callaghan
Lecture
Face to Face On Campus
2 hour(s) per week(s) for 13 week(s) starting Week 1

Workshop
Face to Face On Campus
2 hour(s) per week(s) for 13 week(s) starting Week 1

Unit Weighting Workload
10
Students are required to spend on average 120-140 hours of effort (contact and non-contact) including assessments per 10 unit course.

CONTACTS

Course Coordinator

Callaghan
Dr Saiful Islam
Saiful.Islam@newcastle.edu.au
Consultation: Wednesday 2 pm - 3 pm, Thursday 9 am - 10 am
Additional appointments must be made via email

Teaching Staff

Other teaching staff will be advised on the course Canvas site.

School Office

School of Information and Physical Sciences
SR233, Social Sciences Building
Callaghan
CESE-SIPS-Admin@newcastle.edu.au
+61 2 4921 5513
9am-5pm (Mon-Fri)

SYLLABUS

Course Content

1. Information and number theory, finite fields2. Classical cryptography3. Contemporary symmetric cyphers4. Public key cryptography5. Key management6. Authentication and digital signatures7. Privacy and Privacy Enhancing Technologies8. Advanced topics: Elliptic curve cryptography and homomorphic encryption9. Applications: Privacy in social networks, electronic voting, digital cash

Course Learning Outcomes

On successful completion of this course, students 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

Course Materials

Recommended Text:

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

COMPULSORY REQUIREMENTS

In order to pass this course, each student must complete ALL of the following compulsory requirements:

Contact Hour Requirements:

-

Course Assessment Requirements:

- Assessment 6 - Final examination: Pass requirement 40% - Must obtain 40% in this assessment item to pass the course.

Compulsory Placement and WHS Requirements:

-

SCHEDULE

ASSESSMENTS

This course has 6 assessments. Each assessment is described in more detail in the sections below.

	Assessment Name	Due Date	Involvement	Weighting	Learning Outcomes
1	Mid-term test 1	Week 5	Individual	10%	2
2	Assignment 1	Friday 11:59 PM of Week 6	Pair	10%	1
3	Assignment 2	Friday 11:59 PM of Week 10	Pair	10%	4
4	Mid-Term test 2	Week 12	Individual	20%	2, 3
5	Weekly quizzes	Weekly, 11:59 PM Fridays	Individual	10%	2, 3, 5
6	Final examination*	Exam period	Individual	40%	2, 3, 5

* This assessment has a compulsory requirement.

Late Submissions The mark for an assessment item submitted after the designated time on the due date, without an approved extension of time, will be reduced by 10% of the possible maximum mark for that assessment item for each day or part day that the assessment item is late. Note: this applies equally to week and weekend days.

Assessment 1 - Mid-term test 1

Assessment Type In Term Test
Purpose The purpose and benefit of the class tests is to provide the students with regular feedback on their learning. These tests highlight areas of concern and may stimulate discussion with tutors and lecturers.
Description Written test consisting of short answer questions. The test would last 60 minutes and would take place during the lecture.
Weighting 10%
Due Date Week 5
Submission Method In Class
Assessment Criteria Each question and part of the question is worth specified number of points; to earn the points students must show all the workings and not just the end result.
Return Method In Class
Feedback Provided In Class - Marked papers will be returned to students as soon as possible, and no more than 2 weeks after the test date. Individual feedback is provided within the marked paper; class feedback describing common mistakes, etc., is posted in Canvas.
Opportunity to Reattempt Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 2 - Assignment 1

Assessment Type	Written Assignment
Purpose	To assist deeper understanding of the subject material.
Description	In Assignment 1 students will be presented with a number of ciphertexts encrypted with classical ciphers. Their task will be to break the ciphers and recover the original messages (plaintexts).
Weighting	10%
Due Date	Friday 11:59 PM of Week 6
Submission Method	Online
Assessment Criteria	In order to score marks, students need to describe in detail the process of breaking the ciphers including the strategies followed, concrete steps that lead to the solutions, as well as failed attempts.
Return Method	Online
Feedback Provided	Online - Marked papers will be returned to students as soon as possible, and no more than 32 weeks after the test date. Individual feedback is provided within the marked paper; class feedback describing common mistakes, etc., is posted in Canvas.
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 3 - Assignment 2

Assessment Type	Written Assignment
Purpose	To assist deeper understanding of the subject material.
Description	Design a system that will provide encryption, decryption and authentication.
Weighting	10%
Due Date	Friday 11:59 PM of Week 10
Submission Method	Online
Assessment Criteria	The assessments will be assessed based functionality and quality of the solution.
Return Method	Online
Feedback Provided	Online - Marked papers will be returned to students as soon as possible, and no more than 2 weeks after the test date. Individual feedback is provided in a marking sheet and made available to each student pair separately via Canvas; class feedback describing common mistakes, etc., is posted in Canvas.
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 4 - Mid-Term test 2

Assessment Type	In Term Test
Purpose	The purpose and benefit of the class tests is to provide the students with regular feedback on their learning. These tests highlight areas of concern and may stimulate discussion with tutors and lecturers. Midterm Test 2 will also serve as a preparation for the final exam.
Description	Written test consisting of short answer questions. The test would last 60 minutes and would take place during the lecture.
Weighting	20%
Due Date	Week 12
Submission Method	In Class
Assessment Criteria	Each question and part of the question is worth specified number of points; to earn the points students must show all the workings and not just the end result.
Return Method	In Class
Feedback Provided	In Class - Marked papers will be returned to students as soon as possible, and no more than 2 weeks after the test date. Individual feedback is provided within the marked paper; class feedback describing common mistakes, etc., is posted in Canvas.
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 5 - Weekly quizzes

Assessment Type	Quiz
Purpose	To assist continues learning and provide feedback.
Description	Weekly online quizzes. Multiple choice.
Weighting	10%

Due Date	Weekly, 11:59 PM Fridays
Submission Method	Online
Assessment Criteria	Each question and part of the question is worth specified number of points.
Return Method	Online
Feedback Provided	Online - Immediately. The quizzes are marked automatically in Canvas.
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 6 - Final examination

Assessment Type	Formal Examination
Purpose	The evaluate the students' knowledge and understanding of the subject material.
Description	Exams are designed to test students' knowledge and understanding of the course material and their ability to analyse that material. The exam will include written questions. The duration of the exam would be 2 hours.
Weighting	40%
Compulsory Requirements	Pass requirement 40% - Must obtain 40% in this assessment item to pass the course..
Due Date	Exam period
Submission Method	Formal Exam
Assessment Criteria	Each question and part of the question is worth specified number of points; to earn the points students must show all the workings and not just the end result.
Return Method	Not Returned
Feedback Provided	No Feedback - .
Opportunity to Reattempt	Students WILL be given the opportunity to reattempt this assessment.

ADDITIONAL INFORMATION

Grading Scheme

This course is graded as follows:

Range of Marks	Grade	Description
85-100	High Distinction (HD)	Outstanding standard indicating comprehensive knowledge and understanding of the relevant materials; demonstration of an outstanding level of academic achievement; mastery of skills*; and achievement of all assessment objectives.
75-84	Distinction (D)	Excellent standard indicating a very high level of knowledge and understanding of the relevant materials; demonstration of a very high level of academic ability; sound development of skills*; and achievement of all assessment objectives.
65-74	Credit (C)	Good standard indicating a high level of knowledge and understanding of the relevant materials; demonstration of a high level of academic achievement; reasonable development of skills*; and achievement of all learning outcomes.
50-64	Pass (P)	Satisfactory standard indicating an adequate knowledge and understanding of the relevant materials; demonstration of an adequate level of academic achievement; satisfactory development of skills*; and achievement of all learning outcomes.
0-49	Fail (FF)	Failure to satisfactorily achieve learning outcomes. If all compulsory course components are not completed the mark will be zero. A fail grade may also be awarded following disciplinary action.

*Skills are those identified for the purposes of assessment task(s).

Communication Methods

Communication methods used in this course include:

- Canvas Course Site: Students will receive communications via the posting of content or announcements on the Canvas course site.
- Email: Students will receive communications via their student email account.

- Face to Face: Communication will be provided via face to face meetings or supervision.

Course Evaluation

Each year feedback is sought from students and other stakeholders about the courses offered in the University for the purposes of identifying areas of excellence and potential improvement.

Oral Interviews (Vivas)

As part of the evaluation process of any assessment item in this course an oral examination (viva) may be conducted. The purpose of the oral examination is to verify the authorship of the material submitted in response to the assessment task. The oral examination will be conducted in accordance with the principles set out in the Oral Examination (viva) Procedure. In cases where the oral examination reveals the assessment item may not be the student's own work the case will be dealt with under the Student Conduct Rule.

Academic Misconduct

All students are required to meet the academic integrity standards of the University. These standards reinforce the importance of integrity and honesty in an academic environment. Academic Integrity policies apply to all students of the University in all modes of study and in all locations. For the Student Academic Integrity Policy, refer to https://policies.newcastle.edu.au/document/view-current.php?id=35.

Adverse Circumstances

The University acknowledges the right of students to seek consideration for the impact of allowable adverse circumstances that may affect their performance in assessment item(s). Applications for special consideration due to adverse circumstances will be made using the online Adverse Circumstances system where:

1. the assessment item is a major assessment item; or
2. the assessment item is a minor assessment item and the Course Co-ordinator has specified in the Course Outline that students may apply the online Adverse Circumstances system;
3. you are requesting a change of placement; or
4. the course has a compulsory attendance requirement.

Before applying you must refer to the Adverse Circumstance Affecting Assessment Items Procedure available at:
https://policies.newcastle.edu.au/document/view-current.php?id=236

Important Policy Information

The Help button in the Canvas Navigation menu contains helpful information for using the Learning Management System. Students should familiarise themselves with the policies and procedures at https://www.newcastle.edu.au/current-students/respect-at-uni/policies-and-procedures that support a safe and respectful environment at the University.

GRADUATE PROFILE STATEMENTS

The following table illustrates how this course contributes towards building the skills students will need to work in their profession.

Level of capability

- Level 1 indicates an introduction to a topic at a university level
- Levels 2 and 3 indicate progressive reinforcement of that topic
- Level 4 indicates skills commensurate with a graduate – entry to professional practice
- Level 5 indicates highly specialist or professional ability

Bachelor of Computer Science

	University of Newcastle Bachelor of Computer Science Graduate Profile Statement	Taught	Practised	Assessed	Level of capability
1	Knowledge of basic science and computer science fundamentals				
2	In depth technical competence in the discipline of computer science	X	X	X	3
3	An ability to carry out problem analysis, requirements capture, problem formulation and integrated software development for the solution of a problem	X	X	X	3
4	Capacity to continue developing relevant knowledge, skills and expertise in computer science throughout their careers	X	X	X	3
5	An ability to communicate effectively with other Computer Scientists, Software Engineers, other professional disciplines, managers and the community generally				
6	Ability to undertake and co-ordinate large computer science projects and to identify problems, their formulation and solution				
7	Ability to function effectively as an individual, a team member in multidisciplinary and multicultural teams and as leader/manager with capacity to assist and encourage those under their direction	X	X	X	3
8	Understanding of social, cultural, global and business opportunities of the professional computer scientist; understanding the need for and principles of sustainability and adaptability	X	X	X	3
9	Understanding of professional and ethical responsibilities and a commitment to them	X	X	X	3
10	Understanding of entrepreneurship; need of and process of innovation, as well as the need of and capacity for lifelong learning				

Bachelor of Engineering

	University of Newcastle Bachelor of Engineering Graduate Profile Statements	Taught	Practised	Assessed	Level of capability
	Knowledge Base				
1	1.1. Comprehensive, theory based understanding of the underpinning natural and physical sciences and the engineering fundamentals applicable to the engineering discipline.				
2	1.2. Conceptual understanding of the, mathematics, numerical analysis, statistics, and computer and information sciences which underpin the engineering discipline.	X	X	X	3
3	1.3. In-depth understanding of specialist bodies of knowledge within the engineering discipline.	X	X	X	3
4	1.4. Discernment of knowledge development and research directions within the engineering discipline.	X	X		3
5	1.5. Knowledge of contextual factors impacting the engineering discipline.				
6	1.6. Understanding of the scope, principles, norms, accountabilities and bounds of contemporary engineering practice in the specific discipline.	X	X	X	3
	Engineering Ability				
7	2.1. Application of established engineering methods to complex engineering problem solving.	X	X	X	3
8	2.2. Fluent application of engineering techniques, tools and resources.	X	X	X	3
9	2.3. Application of systematic engineering synthesis and design processes.				
10	2.4. Application of systematic approaches to the conduct and management of engineering projects.				
	Professional Attributes				
11	3.1. Ethical conduct and professional accountability	X	X	X	3
12	3.2. Effective oral and written communication in professional and lay domains.				
13	3.3. Creative, innovative and pro-active demeanour.				
14	3.4. Professional use and management of information.				
15	3.5. Orderly management of self, and professional conduct.	X	X		
16	3.6. Effective team membership and team leadership.	X	X	X	3

This course outline was approved by the Head of School. No alteration of this course outline is permitted without Head of School approval. If a change is approved, students will be notified and an amended course outline will be provided in the same manner as the original.