Faculty of Engineering & Built Environment

School of Electrical Engineering and Computing

COMP3260: Data Security

Callaghan

Semester 1 - 2019

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.

Assumed Knowledge

SENG1110
SENG1120
MATH1510 or equivalent

Contact Hours

Callaghan
Lecture *
Face to Face On Campus
2 hour(s) per Week for Full Term

Workshop
Face to Face On Campus
2 hour(s) per Week for Full Term

* This contact type has a compulsory requirement.

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
Prof Ljiljana Brankovic
Ljiljana.Brankovic@newcastle.edu.au
16054
Consultation: Wednesday 13:00 - 14:00
ES237

Teaching Staff

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

School Office

School of Electrical Engineering and Computing
ICT307
ICT Building
Callaghan
+61 2 4921 5330
9.00am-1.00pm and 2.00pm-5.00pm (Monday to Friday)

SYLLABUS

Course 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

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. Implement a modern cryptosystem

5. Assess privacy in data publishing

Course Materials

Required 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 - Formal Examination: Minimum Grade / Mark Requirement - Students must obtain a specified minimum grade / mark in this assessment item to pass the course. Students whose overall mark in the course is 50% or more, but who score less than 40% in the compulsory item and thus fail to demonstrate the required proficiency, will be awarded a Criterion Fail grade, which will show as FF on their formal transcript. However, students in this position who have scored at least 25% in the compulsory item will be allowed to undertake a supplementary 'capped' assessment in which they can score at most 50% of the possible mark for that item.

Pre-Placement Requirements:

-

SCHEDULE

Week	Week Begins	Topic	Learning Activity	Assessment Due
1	25 Feb	Introduction to Data Security Revision: Groups, rings, fields		
2	4 Mar	Number theory	Game 1	Quiz 1
3	11 Mar	Information theory, perfect secrecy, unicity distance Revision: Probability	Game 2	Quiz 2
4	18 Mar	Classical ciphers	Game 3	Test 1; Quiz 3 Assignment 1 out
5	25 Mar	Stream and block ciphers; Feistel cipher; DES and DES modes of operation	Game 4	Quiz 4
6	1 Apr	AES; AES polynomial arithmetic	Game 5	Quiz 5 Assignment 1 due Assignment 2 out
7	8 Apr	PK Encryption, RSA, ElGamal	Game 6	Quiz 6
Mid Semester Break				
Mid Semester Break				
8	29 Apr	Key management; message authentication	Game 7	Quiz 7
9	6 May	Hash functions and digital signatures	Game 8	Assignment 2 due Quiz 8
10	13 May	Selected topics in cryptography and security	Game 9	Quiz 9
11	20 May	Privacy	Game 10	Quiz 10
12	27 May	Privacy	Game 11	Test 2 Quiz 11
13	3 Jun	No lecture, exam preparation week		
Exam Period				
Exam Period				
Exam Period				

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 4	Individual	10%	2
2	Mid-term test 2	Week 12	Individual	20%	2, 3
3	Assignment 1	Week 6	Pair	10%	1
4	Assignment 2	Week 9	Pair	10%	4
5	Weekly quizzes	Weekly	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
Weighting 10%
Due Date Week 4
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 Returned Work - Marked papers will be returned to students as soon as possible, and no more than 3 weeks after the test date..

Assessment 2 - 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
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 Returned Work - Marked papers will be returned to students as soon as possible, and no more than 3 weeks after the test date.. Individual feedback is provided within the marked paper; class feedback describing common mistakes, etc., is posted in Blackboard.

Assessment 3 - 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	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 3 weeks after the test date.. Individual feedback is provided within the marked paper; class feedback describing common mistakes, etc., is posted in Blackboard.

Assessment 4 - Assignment 2

Assessment Type	Written Assignment
Purpose	To assist deeper understanding of the subject material.
Description	In assignment 2 the students will work in pairs to implement one of the modern cryptosystems.
Weighting	10%
Due Date	Week 9
Submission Method	Online
Assessment Criteria	The assessments will be assessed based on correctness of the code, as well as code readability.
Return Method	Not Returned
Feedback Provided	Online - Marked papers will be returned to students as soon as possible, and no more than 3 weeks after the test date.. Individual feedback is provided in a marking sheet and made available to each student pair separately via Blackboard; class feedback describing common mistakes, etc., is posted in Blackboard.

Assessment 5 - Weekly quizzes

Assessment Type	Quiz
Purpose	To assist continues learning and provide feedback.
Description	Weekly online quizzes.
Weighting	10%
Due Date	Weekly
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 Blackboard..

Assessment 6 - Final examination

Assessment Type	Formal Examination
Purpose	The evaluate the students' knowledge and understanding of the subject material.
Description	
Weighting	40%
Compulsory Requirements	Minimum Grade / Mark Requirement - Students must obtain a specified minimum grade / mark 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. Refer to course outline for details.

Bachelor of Computer Science

	University of Newcastle Bachelor of Computer Science Graduate Profile Statements	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**

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:

- Blackboard Course Site: Students will receive communications via the posting of content or announcements on the Blackboard course site.
- 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.

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

You are entitled to apply for special consideration because adverse circumstances have had an impact on your performance in an assessment item. This includes applying for an extension of time to complete an assessment item. Prior to applying you must refer to the Adverse Circumstances Affecting Assessment Items Procedure, available at https://policies.newcastle.edu.au/document/view-current.php?id=236. All applications for Adverse Circumstances must be lodged via the online Adverse Circumstances system, along with supporting documentation.

Important Policy Information

The 'HELP for Students' tab in UoNline contains important information that all students should be familiar with, including various systems, policies and procedures.

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.