

Course Outline

Code: SEC604

Title: Cryptography, Blockchain and Security

Faculty:	Science, Health, Education & Engineering
School:	Science & Engineering
Teaching Session:	Semester 2
Year:	2019
Course Coordinator:	Dennis Desmond
Course Moderator:	Professor David Lacey

Please go to the USC website for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1 Description

A cyber security specialist will use a complex array of tools, methods and applications to investigate and protect information in computer systems. This online course has been designed to introduce you to some cryptography techniques that allow different parties to securely transmit information. The course will introduce blockchain and its growing uses, including cryptocurrencies. You will learn the differences between authentication and security protocols and how private keys are exchanged to establish secure communications.

1.2 Field trips, WIL placements or activities required by professional accreditation

Activity	Details
Nil	Nil

2. What level is this course?

600 level Specialised - Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

Specific Learning Outcomes On successful completion of this course, you should be able to:	Assessment tasks You will be assessed on the learning outcomes in task/s:	Graduate Qualities or Professional Standards mapping Completing these tasks successfully will contribute to:
Identify and explain the evolution of cryptographic protocols.	1	Knowledgeable
Explain the cryptographic function of block ciphers and their value in proving the authenticity of data transactions.	1	Knowledgeable
Identify and discuss the elements of the key exchange process.	2	Knowledgeable
Apply a range of security applications suitable to secure a network connected device.	2	Empowered
Compare and contrast the value to data security and privacy of cryptographic protocols outlining their strengths and vulnerabilities.	2	Empowered
Demonstrate the qualities of professionalism , leadership and digital collaboration.	2	Engaged
Communicate research and findings to specialist and non-specialist audiences.	1,2,	Engaged

5. Am I eligible to enrol in this course?

Refer to the [USC Glossary of terms](#) for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1 Enrolment restrictions

Nil

5.2 Pre-requisites

Nil

5.3 Co-requisites

Nil

5.4 Anti-requisites

Nil

5.5 Specific assumed prior knowledge and skills (where applicable)

Students will be assumed to understand technology and its role in society. They will be expected to have a working knowledge of computer systems and networks

6. How am I going to be assessed?

6.1 Grading scale

Standard – High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL)

6.2 Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment during tutorials

6.3 Assessment tasks

Task No.	Assessment Product	Individual or Group	Weighting %	What is the duration / length?	When should I submit?	Where should I submit it?
1	Report	Individual	40%	1500	Week 5	Online Assignment Submission with Plagiarism check
2	Case Study	Group	30%	1000	Week 10	Online Assignment Submission with Plagiarism check
3	Essay	Individual	30%	2000	Week 13	Online Assignment Submission with Plagiarism check
			100%			

Assessment Task 1: The blockchain game changer

Goal:	The goal of this task is to understand blockchain technology and its role in cybercrime methodologies and you will examine the reasons why blockchain technology is perceived as a trusted form of online authentication.
Product:	Case Study
Format:	You will prepare a written report showing your understanding of the emergence of blockchain technology and its use in society today. You will also demonstrate an understanding of the protocols used in blockchain technology and its uses in demonstrating the authenticity of communications.
Criteria:	<ul style="list-style-type: none"> • Demonstration of understanding of the blockchain technology • Explanation of applications • Evaluation of 'trustworthiness' • Professional communication

Assessment Task 2: Digital group cryptology challenge

Goal:	This is a cryptology challenge task where you will work with a team to decipher and work through a complex case study. The goal of this task is to understand the differences between cryptographic and data authentication protocols and to understand the key exchange protocol and its relevance to the security of communication.
Product:	Report
Format:	You will prepare a written report as a group identifying the features of cryptographic and authentication protocols. You will compare and contrast their features and discuss their roles in data privacy and authentication. The report will have an annex that outlines the work of the team members, specific elements/roles performed by the members and an indication of the division of work.
Criteria:	<ul style="list-style-type: none"> • Identification of the elements of cryptographic and authentication protocols. • Comparison of the features of cryptographic and authentication protocols. • Discussion - different roles both play in data security and authentication. • Communication • Collaboration

Assessment Task 3: The Right to Encrypt for Privacy and Security versus the Right for Governments to Decrypt

Goal:	The goal of this essay is to demonstrate your knowledge of key arguments for and against Government decryption powers and to argue a clear position backed by evidence. This will demonstrate your ability to apply key concepts to real world scenarios, including the practical challenges in applying decryption key laws within an encryption context.
Product:	Essay (Individual not Group)
Format:	You will submit a 2000-word limit essay to address the position as to whether you are in favour of recently introduced Australian (Commonwealth) decryption laws. Your essay must cover key concepts, stakeholder positions, the mechanics of the law and its “practical” workability, and consider a clear position of support or not for these legislative changes and evidence to support your position.
Criteria:	<p>The essay paper will be assessed by the degree of achievement in the following areas:</p> <ul style="list-style-type: none"> • Argues a clear, consistent case to answer a position for or against decryption laws. • Correctly applies relevant encryption theories and frameworks. • Multiple perspectives are presented and arguments made on different sides and relevant position(s). • Scholarly and authoritative reference sources are used to directly support claims and arguments. • Demonstrates critical thinking, analysis and synthesis of argument. • Sentence and paragraph structures are clear and absent of grammatical and typographical errors. • Correctly uses the APA Style of referencing with a List of References (LORs) at the end. • Will be +/- 10 percent of the stated word count.

7. What are the course activities?

7.1 Directed study hours

The directed study hours listed here are a portion of the workload for this course. A 12 unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Directed study hours may vary by location. Student workload is calculated at 12.5 learning hours per one unit.

Location:	Directed study hours for location:
Online	This online course will take between 10-12 hours per week and may include a combination of: webinar, peer to peer collaboration, asynchronous online materials, and synchronous lecturer and peer to peer zoom meetings.

7.2 Course content

Week # / Module #	What key concepts/content will I learn?
1 The world of Cryptology, Cryptography and Cryptanalysis	The history and development of cryptography, the theory of codes and ciphers, and Public and Private Key encryption, crypto protocols, and hash functions.
2 The fundamentals and strategy of Blockchain	Blockchain essentials, cryptocurrencies and their supporting infrastructure, the onion network and TOR, cryptomarkets and peer to peer marketplaces
3 Security and applications	Commercial encryption applications and tools, certificates, steganography, and Internet security protocols. Privacy and security, specialised communications, and encryption use by adversaries

4 The policy, law and rights when it comes to encryption	The relationship and disconnect between fundamental rights to privacy and security and their enablement through encryption versus the rights of Government agencies to decrypt and the established policy positions of Nation-States.
5. The future of cryptography, encryption and security	Students will learn what security mean in a world of increasing use of biometrics and the digitisation of identity information. They will use their accumulated knowledge of the course to challenge established views and thinking around encryption and decryption and the linking of these to a person's biological footprint.

8. What resources do I need to undertake this course?

Please note that course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Blackboard site. Please log in as soon as possible.

8.1 Prescribed text(s) or course reader

Please note that you need to have regular access to the resource(s) listed below as they are required:

Author	Year	Title	Publisher
Kahn, D.	1996	<i>The Codebreakers: The comprehensive history of secret communication from ancient times to the internet.</i>	Simon and Schuster.
Ling Ngo, D.C., Jin Teoh, A. B., & Hu, J.	2015	<i>Biometric Security</i>	Cambridge Scholars Publishing.

8.2 Specific requirements

This is an online course therefore access to a computer and the internet for 10-12 hours per week is essential.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low.

It is your responsibility as a student to review course material, search online, discuss with lecturers and peers, and understand the health and safety risks associated with your specific course of study. It is also your responsibility to familiarise yourself with the University's general health and safety principles by reviewing the [online Health Safety and Wellbeing training module for students](#), and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1 Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

10.2 Assessment: Additional requirements

Eligibility for Supplementary Assessment

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:

- a) The final mark is in the percentage range 47% to 49.4%
- b) The course is graded using the Standard Grading scale
- c) You have not failed an assessment task in the course due to academic misconduct

10.3 Assessment: Submission penalties

Late submission of assessment tasks will be penalised at the following maximum rate:

- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.
- 10% (of the assessment task's identified value) for the third day
- 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.
- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task.

Weekdays and weekends are included in the calculation of days late.

To request an extension, you must contact your Course Coordinator and supply the required documentation to negotiate an outcome.

10.4 Study help

In the first instance, you should contact your tutor, then the Course Coordinator. Additional assistance is provided to all students through Academic Skills Advisers. To book an appointment or find a drop-in session go to [Student Hub](#). Contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au

10.5 Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website:

<http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching>

10.6 General Enquiries

In person:

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **USC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **USC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au