



COURSE OUTLINE

SEC604 Cryptography, Blockchain and Security

Course Coordinator: Dennis Desmond (ddesmond@usc.edu.au) **School:** School of Science, Technology and Engineering

2021 | Semester 2

Online

ONLINE

You can do this course without coming onto campus.

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. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
ONLINE 1			
Tutorial/Workshop 1 – a weekly tutorial is offered online each week	1hr	Week 1	13 times
Lecture – Course Content is provided via Sway and Blackboard with proof of work assignments and written assessments to be emailed to course coordinator	5hrs	Week 1	13 times

1.3. Course Topics

- History and Cryptography Concepts
- Crypto and data authentication protocols
- Encryption as a Weapon
- Legal, Policy and Ethics Framework of Encryption
- Commercial Encryption Tools
- Blockchain
- The Onion Network and TOR
- Cryptocurrencies and Cryptocurrency Support
- SSL/TLS and HTTPS, Certificates
- Steganography and Secret Writing
- Virtual Private Networks and Secure Peer to Peer Networks
- Communications Security Principles

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?

COURSE LEARNING OUTCOMES	GRADUATE QUALITIES
On successful completion of this course, you should be able to...	Completing these tasks successfully will contribute to you becoming...
1 Identify and explain the evolution of cryptographic protocols.	Knowledgeable
2 Explain the cryptographic function of block ciphers and their value in proving the authenticity of data transactions.	Knowledgeable
3 Identify and discuss the elements of the key exchange process.	Knowledgeable
4 Apply a range of security applications suitable to secure a network connected device.	Empowered
5 Compare and contrast the value to data security and privacy of cryptographic protocols outlining their strengths and vulnerabilities.	Empowered
6 Demonstrate the qualities of professionalism, leadership and digital collaboration.	Engaged
7 Communicate research and findings to specialist and non-specialist audiences.	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. Pre-requisites

Enrolled in SC509, SC517 or BU708

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. 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 Grading (GRD)

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

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Report	Individual	40%	1500 words	Week 5	Online Assignment Submission with plagiarism check
All	2	Case Study	Group	30%	1000 words	Week 10	Online Assignment Submission with plagiarism check
All	3	Essay	Individual	30%	2000 words (+/- 10 percent of the stated word count)	Week 13	Online Assignment Submission with plagiarism check

All - 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:	Report																
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:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Demonstration of understanding of the blockchain technology</td> <td>1 2</td> </tr> <tr> <td>2</td> <td>Explanation of applications</td> <td>1</td> </tr> <tr> <td>3</td> <td>Evaluation of 'trustworthiness'</td> <td>1</td> </tr> <tr> <td>4</td> <td>Professional communication</td> <td>7</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Demonstration of understanding of the blockchain technology	1 2	2	Explanation of applications	1	3	Evaluation of 'trustworthiness'	1	4	Professional communication	7	
No.		Learning Outcome assessed															
1	Demonstration of understanding of the blockchain technology	1 2															
2	Explanation of applications	1															
3	Evaluation of 'trustworthiness'	1															
4	Professional communication	7															

All - 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:	Case Study
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:	No.	Learning Outcome assessed
	1	Identification of the elements of cryptographic and authentication protocols ②
	2	Comparison of the features of cryptographic and authentication protocols. ②
	3	Discussion - different roles both play in data security and authentication ③
	4	Professional communication of case study findings ⑦
	5	Demonstrate effective team work and professionalism within the team ⑥

All - 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	
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:	No.	Learning Outcome assessed
	1	Argues a clear, consistent case to answer a position for or against decryption laws ⑤
	2	Correctly applies relevant encryption theories and frameworks ①
	3	Multiple perspectives are presented and arguments made on different sides and relevant position(s) ④
	4	Scholarly and authoritative reference sources are used to directly support claims and arguments ⑦
	5	Demonstrates critical thinking, analysis and synthesis of argument ⑤
	6	Sentence and paragraph structures are clear and absent of grammatical and typographical errors ⑦
	7	Correctly uses the APA Style of referencing with a List of References (LORs) at the end ⑦

7. Directed study hours

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.

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

Please note: 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. Resources may be required or recommended.

REQUIRED?	AUTHOR	YEAR	TITLE	PUBLISHER
Required	Kahn, D.	1996	The Codebreakers: The comprehensive history of secret communication from ancient times to the internet.	Simon and Schuster.
Required	Ling Ngo, D.C., Jin Teoh, A. B., & Hu, J.	2015	Biometric Security	Cambridge Scholars Publishing.

8.2. Specific requirements

This is an online course therefore access to a computer with systems admin rights and unrestricted access to 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 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 and to familiarise yourself with the University's general health and safety principles by reviewing the [online induction training 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

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

The final mark is in the percentage range 47% to 49.4%

The course is graded using the Standard Grading scale

You have not failed an assessment task in the course due to academic misconduct.

10.3. Assessment: Submission penalties

Late submission of assessment tasks may 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 to negotiate an outcome.

10.4. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the [Learning Advisers](#) web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

10.5. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to [Student Hub](#), email studentwellbeing@usc.edu.au or call 07 5430 1226.

10.6. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, , injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, [AccessAbility Services](#) can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to [Student Hub](#), email AccessAbility@usc.edu.au or call 07 5430 2890.

10.7. 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>

10.8. General Enquiries

In person:

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **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
- **USC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au