

SEC604 Cryptography, Blockchain and Security

School: School of Science, Technology and Engineering

2026 | Trimester 2

UniSC Sunshine Coast
UniSC Adelaide

**BLENDED
LEARNING**

Most of your course is on campus but you may be able to do some components of this course online.

Online

ONLINE

You can do this course without coming onto campus, unless your program has specified a mandatory onsite requirement.

Please go to unisc.edu.au 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
BLENDED LEARNING			
Learning materials – Asynchronous learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous on campus workshop	2hrs	Week 1	12 times
Seminar – On campus seminar	1hr	Week 1	2 times
ONLINE			
Learning materials – Asynchronous learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous Zoom workshop	2hrs	Week 1	12 times
Seminar – Online seminar	1hr	Week 1	2 times

1.3. Course Topics

1. Introduction to Cryptography
2. Legal, Policy and Ethics Framework of Encryption
3. Network data authentication protocols
4. Commercial Encryption Tools
5. Communications Security Principles
6. SSL/TLS and HTTPS, Certificates
7. Steganography and Secret Writing
8. Virtual Private Networks and Secure Peer to Peer Networks
9. The Onion Network and TOR
10. Introduction to Blockchain
11. Introduction to cryptocurrencies
12. Developing technologies in Cryptography

1.4. Mature Content

Drug Use, Sex/Sexual references, Violence

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

5.1. Pre-requisites

SEC601 and Enrolled in SC509, SC705, 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

5.5. Microcredential Information

Not applicable

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	Artefact - Technical and Scientific, and Written Piece	Individual	40%	2,500 words (+/- 10 percent of the stated word count)	Week 5	Online Assignment Submission with plagiarism check
All	2	Artefact - Technical and Scientific, and Written Piece	Individual	40%	2,000 words (+/- 10 percent of the stated word count)	Week 9	Online Assignment Submission with plagiarism check
All	3	Portfolio	Individual	20%	1000 words equivalent	Week 12	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Cryptographic evaluation.

GOAL:	This written piece will evaluate a cyber security case study of a company and identify proper encryption and cryptographic approaches to security.																						
PRODUCT:	Artefact - Technical and Scientific, and Written Piece																						
AUTHORSHIP STATEMENT:																							
FORMAT:	Students will prepare a written report of no more than 2,500 words using APA7 referencing style. The artefact will be written in Australian English and provide suitable information that a technical and non technical person may understand.																						
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Describes protocols and processes in use within a company and their effectiveness</td> <td>5</td> </tr> <tr> <td>2</td> <td>Correctly applies relevant encryption theories and frameworks</td> <td>1</td> </tr> <tr> <td>3</td> <td>Multiple perspectives are presented and arguments made on different sides and relevant position(s)</td> <td>4</td> </tr> <tr> <td>4</td> <td>Scholarly and authoritative reference sources using APA style referencing are used to directly support claims and arguments</td> <td>7</td> </tr> <tr> <td>5</td> <td>Demonstrates critical thinking, analysis and synthesis of argument</td> <td>5</td> </tr> <tr> <td>6</td> <td>Sentence and paragraph structures are clear and absent of grammatical and typographical errors</td> <td>7</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Describes protocols and processes in use within a company and their effectiveness	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 using APA style referencing 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	
No.		Learning Outcome assessed																					
1	Describes protocols and processes in use within a company and their effectiveness	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 using APA style referencing 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																					
GENERIC SKILLS:	Communication, Problem solving, Organisation, Applying technologies, Information literacy																						

All - Assessment Task 2: Cryptographic technical review.

GOAL:	This is a cryptographic task where you will individually work through a complex case study.																			
PRODUCT:	Artefact - Technical and Scientific, and Written Piece																			
AUTHORSHIP STATEMENT:																				
FORMAT:	Students will prepare a written report of no more than 2,000 words using APA7 referencing style. The artefact will be written in Australian English and provide suitable information that a technical and non technical person may understand.																			
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Identification of the elements of cryptographic and authentication protocols</td> <td>2</td> </tr> <tr> <td>2</td> <td>Comparison of the features of cryptographic and authentication protocols.</td> <td>2</td> </tr> <tr> <td>3</td> <td>Discussion - different roles both play in data security and authentication</td> <td>3</td> </tr> <tr> <td>4</td> <td>Professional communication of case study findings</td> <td>7</td> </tr> <tr> <td>5</td> <td>Demonstrate effective team work and professionalism within the team</td> <td>6</td> </tr> </tbody> </table>	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	
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																		
GENERIC SKILLS:	Communication, Problem solving, Organisation, Applying technologies, Information literacy																			

All - Assessment Task 3: Proof of Work Portfolio

GOAL:	Students will complete cryptography related tasks demonstrating their understanding and knowledge of encryption and cryptographic protocols by performing periodic practical tasks.																
PRODUCT:	Portfolio																
AUTHORSHIP STATEMENT:																	
FORMAT:	Word document individually submitted online via LMS.																
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Demonstrate understanding of cryptographic protocols and encryption</td> <td>1</td> </tr> <tr> <td>2</td> <td>Evaluation of privacy, security, reliability</td> <td>1 4 5 7</td> </tr> <tr> <td>3</td> <td>Professional communication</td> <td>7</td> </tr> <tr> <td>4</td> <td>Describe practical applications of encryption applications</td> <td>2 4 5 7</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Demonstrate understanding of cryptographic protocols and encryption	1	2	Evaluation of privacy, security, reliability	1 4 5 7	3	Professional communication	7	4	Describe practical applications of encryption applications	2 4 5 7	
No.		Learning Outcome assessed															
1	Demonstrate understanding of cryptographic protocols and encryption	1															
2	Evaluation of privacy, security, reliability	1 4 5 7															
3	Professional communication	7															
4	Describe practical applications of encryption applications	2 4 5 7															
GENERIC SKILLS:	Communication, Problem solving, Organisation, Applying technologies, Information literacy																

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. 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 Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

You need regular access to the resource(s) below. Many texts are available as ebooks through the [Library](#) at no additional cost.

REQUIRED?	AUTHOR	YEAR	TITLE	EDITION	PUBLISHER
Recommended	David Kahn	1996	The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet	n/a	Scribner
Recommended	David Gerard	2017	Attack of the 50 Foot Blockchain	n/a	David Gerard
Recommended	Robert Wallace,H. Keith Melton	2009	Spycraft	n/a	Penguin
Recommended	Daniel Drescher	2017	Blockchain Basics	n/a	Apress

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 Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

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%; and
- (b) The course is graded using the Standard Grading scale

10.3. Assessment: Submission penalties

Late submissions may be penalised up to and including the following maximum percentage of the assessment task's identified value, with weekdays and weekends included in the calculation of days late:

- (a) One day: deduct 5%;
- (b) Two days: deduct 10%;
- (c) Three days: deduct 20%;
- (d) Four days: deduct 40%;
- (e) Five days: deduct 60%;
- (f) Six days: deduct 80%;
- (g) Seven days: A result of zero is awarded for the assessment task.

The following penalties will apply for a late submission for an online examination:

Less than 15 minutes: No penalty

From 15 minutes to 30 minutes: 20% penalty

More than 30 minutes: 100% penalty

10.4. 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
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit <https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching>

10.5. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The [Student Charter](#) sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.6. General Enquiries

In person:

- **UniSC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **UniSC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **UniSC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **UniSC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **UniSC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **UniSC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au

