

**SEC304**

# Cryptography, Blockchain and Information Security

**School:** School of Science, Technology and Engineering

2024 Semester 2

UniSC Moreton Bay

**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.

Please go to [usc.edu.au](http://usc.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

Cyber security specialist will use a complex array of tools, methods and applications to investigate and protect information in computer systems. You will be introduced to cryptography techniques that allow different parties to securely transmit information. You will explore 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 |
|--|-------|----------------|-----------|
| <b>BLENDED LEARNING</b>                                    |       |                |           |
| <b>Learning materials</b> – Asynchronous learning material | 2hrs  | Week 1         | 13 times  |
| <b>Tutorial/Workshop 1</b> – On campus workshop            | 2hrs  | Week 1         | 13 times  |
| <b>ONLINE</b>  |       |                |           |
| <b>Learning materials</b> – Asynchronous learning material | 2hrs  | Week 1         | 13 times  |
| <b>Tutorial/Workshop 1</b> – Online workshop               | 2hrs  | Week 1         | 13 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

## 2. What level is this course?

300 Level (Graduate)

Demonstrating coherence and breadth or depth of knowledge and skills. Independent application of knowledge and skills in unfamiliar contexts. Meeting professional requirements and AQF descriptors for the degree. May require pre-requisites where discipline specific introductory or developing knowledge or skills is necessary. Normally undertaken in the third or fourth full-time study year of an undergraduate program.

## 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 Demonstrate knowledge of cryptography fundamentals for security and authentication.                                      | Knowledgeable  |
| 2 Compare and contrast data security and privacy of cryptographic protocols outlining their strengths and vulnerabilities. | Creative and critical thinker  |
| 3 Demonstrate the qualities of professionalism, leadership and digital collaboration.                                      | Engaged  |
| 4 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

SEC301

### 5.2. Co-requisites

Not applicable

### 5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

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

On-going formative feedback will be provided in workshops throughout the course.

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          | 30%         | 2,000 words                                       | Week 5                | Online Assignment Submission with plagiarism check |
| All           | 2        | Case Study   | Group               | 30%         | Written report, maximum of 2,000 words in length. | Week 9                | Online Assignment Submission with plagiarism check |
| All           | 3        | Portfolio  | Individual          | 40%         | Work is performed over the course of the 13 weeks | Exam Period           | Online Assignment Submission with plagiarism check |

All - Assessment Task 1: Network Encryption Protocols

| <b>GOAL:</b>  | This written piece will evaluate the network encryption protocols implemented by a notional company that has been the victim of a data breach. The written piece will provide corporate leadership an assessment of their security status and make specific recommendations to their current business practices and processes.  |     |                           |  |   |  |   |                              |   |   |       |  |
|---|---|-----|---------------------------|--|---|--|---|------------------------------|---|---|-------|--|
| <b>PRODUCT:</b>   | Artefact - Technical and Scientific, and Written Piece  |     |                           |  |   |  |   |                              |   |   |       |  |
| <b>FORMAT:</b>  | Students will prepare a written report of no more than 2,000 words using APA7 style, and then present their concept through an oral presentation. The artefact will be written in plain English and provide suitable information that a non technical person may understand.  |     |                           |  |   |  |   |                              |   |   |       |  |
| <b>CRITERIA:</b>  | <table border="1"> <thead> <tr> <th>No.</th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1 Demonstration of understanding of the encryption protocols</td> <td>1</td> </tr> <tr> <td>2 Explanation of encryption applications</td> <td>1</td> </tr> <tr> <td>3 Professional communication</td> <td>4</td> </tr> <tr> <td>4 Understanding of a practical application for an innovative technology</td> <td>1 2 4</td> </tr> </tbody> </table> | No. | Learning Outcome assessed | 1 Demonstration of understanding of the encryption protocols | 1 | 2 Explanation of encryption applications | 1 | 3 Professional communication | 4 | 4 Understanding of a practical application for an innovative technology | 1 2 4 |  |
| No.   | Learning Outcome assessed   |     |                           |  |   |  |   |                              |   |   |       |  |
| 1 Demonstration of understanding of the encryption protocols            | 1   |     |                           |  |   |  |   |                              |   |   |       |  |
| 2 Explanation of encryption applications                                | 1   |     |                           |  |   |  |   |                              |   |   |       |  |
| 3 Professional communication  | 4   |     |                           |  |   |  |   |                              |   |   |       |  |
| 4 Understanding of a practical application for an innovative technology | 1 2 4   |     |                           |  |   |  |   |                              |   |   |       |  |
| <b>GENERIC SKILLS:</b>  | Communication, Problem solving, Applying technologies, Information literacy   |     |                           |  |   |  |   |                              |   |   |       |  |

### All - Assessment Task 2: Digital group cryptology challenge

|                        |   |  |
|------------------------|---|--|
| <b>GOAL:</b>           | This is a cryptology challenge task where you will work with a team to decipher and work through a complex case study.<br><br>The intent is to examine a case wherein subjects are accused of illicitly removing encrypted information from their workspace and identify the methods and procedures in place that impacted the case.  |  |
| <b>PRODUCT:</b>        | Case Study  |  |
| <b>FORMAT:</b>         | You will prepare a written report as a group identifying the methods by which individuals circumvented security controls to illicitly remove classified information. You will compare and contrast the security features in place and discuss their roles in the securing and protection of protected data. 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. |  |
| <b>CRITERIA:</b>       | <b>No.</b>  | <b>Learning Outcome assessed</b>   |
|                        | 1   | Identification of the elements of cryptographic and authentication protocols 1 |
|                        | 2   | Comparison of the features of cryptographic and authentication protocols. 1    |
|                        | 3   | Discussion - different roles both play in data security and authentication 1   |
|                        | 4   | Professional communication 4   |
|                        | 5   | Demonstrate effective team work and professionalism within the team 3          |
| <b>GENERIC SKILLS:</b> | Communication, Collaboration, Problem solving, Organisation, Applying technologies, Information literacy  |  |

### All - Assessment Task 3: Practical Proof of Work Portfolio

|                        |  |  |
|------------------------|--|--|
| <b>GOAL:</b>           | The goal of this portfolio is to prove knowledge and understanding of cryptographic concepts such as digital wallet creation, revealing steganographic content, creating and decrypting messages |  |
| <b>PRODUCT:</b>        | Portfolio  |  |
| <b>FORMAT:</b>         | Individual proofs of work are emailed to the instructor during each week they are created  |  |
| <b>CRITERIA:</b>       | <b>No.</b>   | <b>Learning Outcome assessed</b>   |
|                        | 1  | Correctly applies relevant encryption theories and frameworks 1  |
|                        | 2  | Understands and demonstrates a practical knowledge of blockchain technologies, cryptofinance concepts, and alternative financial systems 1 4 |
|                        | 3  | Applied theoretical knowledge to a practical application 1 2 4   |
| <b>GENERIC SKILLS:</b> | 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

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             | EDITION | PUBLISHER          |
|-----------|-----------------|------|-------------------|---------|--------------------|
| Required  | David Kahn      | 1996 | The Codebreakers  | n/a     | Simon and Schuster |
| Required  | Daniel Drescher | 2017 | Blockchain Basics | 1st     | Apress             |

## 8.2. Specific requirements

This course requires access to computers and specialised software that are not available at UniSC. Students should have systems administrative level access to be able to install a variety of software applications. If you elect to do this course online, you may either; attend a campus at which it is available, discuss alternative solutions with your course coordinator that would enable you to demonstrate the learning outcomes, or if you prefer you may acquire this software (if necessary at your own expense). Some software providers may offer discounted or free academic licensing.

## 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:

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. SafeUniSC

UniSC is committed to a culture of respect and providing a safe and supportive environment for all members of our community. For immediate assistance on campus contact SafeUniSC by phone: [07 5430 1168](tel:0754301168) or using the [SafeZone](#) app. For general enquires contact the SafeUniSC team by phone [07 5456 3864](tel:0754563864) or email [safe@usc.edu.au](mailto:safe@usc.edu.au).

The SafeUniSC Specialist Service is a Student Wellbeing service that provides free and confidential support to students who may have experienced or observed behaviour that could cause fear, offence or trauma. To contact the service call [07 5430 1226](tel:0754301226) or email [studentwellbeing@usc.edu.au](mailto:studentwellbeing@usc.edu.au).

## 10.5. 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](mailto:studentcentral@usc.edu.au).

## 10.6. 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](mailto:studentwellbeing@usc.edu.au) or call 07 5430 1226.

## 10.7. 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](mailto:AccessAbility@usc.edu.au) or call 07 5430 2890.

## 10.8. 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>

## 10.9. 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.

## 10.10. 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](mailto:studentcentral@usc.edu.au)