

## CSI2108–Cryptographic Concepts

### Portfolio Assignment Part 1 (25%)

**DUE DATE: 25 Feb 2022, Friday 17:00PM**

In the workshops throughout this semester we will learn about and explore various cryptographic concepts and algorithms. As part of this process we will investigate how to make ciphers more secure and how they can be attacked, and the advantages and disadvantages of different kinds of codes and ciphers.

This assignment asks you to formalise your workshop tasks into a **portfolio of cryptographic algorithms**. You will be building several different algorithms in the program(s) of your choice, documenting and explaining your design choices, and critiquing the ciphers you have built.

In this assignment, the focus is not necessarily on building the best possible ciphers, but about being thoughtful and deliberate about your choices. It is about being able to explain and justify your choices, and about demonstrating an understanding of the strengths and weaknesses of the ciphers you have created.

**The portfolio assignment may be completed in groups of 1-3 people.** You will be asked to submit a document stating who you are working with by the end of Week 4 (including if you are working alone). After this date it will not be possible to change groups except to change to an individual assignment. Assignment requirements are the same for all group sizes.

**This document describes Part 1 of the Portfolio, which is worth 25 marks. It focuses on the concepts in Modules 2-5 (stream ciphers and block ciphers). Submission is due in Week 7, and you can request feedback on your work in the two weeks prior to the deadline. Grades and feedback for Part 1 will be given in Week 9.**

To get started on this assignment, read the [Portfolio Part 1 instructions](#) and [Submission instructions](#) below, making note of the mark distribution for each question and what is expected of you. Make sure you read through the advice on [academic integrity](#) to be sure what is acceptable in this assignment and where to get help if you need advice. Post in the Blackboard discussion board if you have any questions.

## PORTFOLIO ASSIGNMENT INSTRUCTIONS PART 1 (25 MARKS)

This section of the Portfolio concentrates on symmetric ciphers. These are generally fast to run and are excellent for encrypting messages.

Complete the following tasks in the programming language of your choice. (This includes MS Excel.) In your video you must demonstrate **HOW** your ciphers operate, i.e. how they take the plaintext and convert it into the ciphertext (including your code and formulas), and **WHAT** each of your design choices were. The accompanying documentation should go into more detail answering **WHY** you made these design choices and discussing the security of your ciphers.

The message X is as follows:

X = "Meet Alice next to the fridge in Building 18 at ECU Joondalup campus."

1. (Week 2) **Design your own stream cipher to encrypt the message X.** (8 MARKS)  
In your documentation/video:
  - Demonstrate how you created the keystream and how you used this to generate the ciphertext. (2 marks)
  - Discuss why you generated the keystream the way that you did. (3 marks: 1 mark for a poor explanation; 2 marks for a good explanation; 3 marks for an excellent explanation that demonstrates thoughtful reasoned choices)
  - Explain or demonstrate how Bob will decrypt Alice's message. (1 mark)
  - Discuss how secure you think your stream cipher is, and why. (2 marks)
2. (Weeks 3-5) **Design your own block cipher to encrypt the message X.** (10 MARKS)  
**Your block cipher should have a block size of 6 or more and should include elements of substitution, permutation and key addition along with multiple rounds of encryption.**  
In your documentation/video:
  - Demonstrate and explain the structure of your block cipher, including how your cipher achieves the properties of confusion and diffusion. (3 marks)
  - State the mode of operation you used to implement your block cipher and discuss the reasons why you chose this method. (3 marks)
  - Discuss how you could make your block cipher more secure. (4 marks: 1 mark for each item (and justification) to increase security above and beyond the specification)
3. **Compare and contrast your two symmetric ciphers.** (7 MARKS)
  - Discuss which cipher you found easier to create or faster to run and why. (1 mark)
  - Discuss which cipher you think is more secure, and why. (2 marks)
  - Compare your stream cipher with Trivium and your block cipher with AES. What features do these ciphers have which make them more secure than your ciphers? (2 marks: 1 mark per cipher)
  - For each of your two ciphers, give an example of a context/situation where that cipher would be more appropriate than the other cipher, and explain why. (2 marks)

## SUBMISSION INSTRUCTIONS (Part 1)

When you create the list of members of your group, you will be asked to nominate one person to be the Group Leader. **Submission of both parts of the Portfolio should only done by the Group Leader.**

The submission requirements for Part 1 of the Portfolio are as follows:

- 1000-word document (.pdf or .docx format) addressing all tasks. This should be submitted via the relevant Turnitin link on Blackboard. (The word count is a guideline. There is no penalty for going above or below it.)
- A 5-minute video explaining the algorithms you have created. Any code you created must be shown and demonstrated in action (this includes formulas in cells if you are using Excel or the code and running of code in Python). All members of the group must speak and be on camera in this video at some point. Each member of the group needs to show photo ID to the camera (e.g. student card, driving licence, passport). This video should be submitted via the “Portfolio video submission” link on Blackboard.

## REFERENCING

The **entirety of your assignment must be your own work or that of your group members**, and any ideas taken from sources outside of the lecture slides must be referenced and paraphrased. All sources of references must be cited (in-text citation) and listed (end reference list). This includes any images you have used that you have not created yourself. If you do not reference correctly or if you are found to be plagiarising others’ work, the assessment will be reported to the Academic Integrity area for investigation. All assignments will be subjected to checks for academic integrity – you can also check this yourself by consulting the Turnitin similarity report before your final submission.

For details about referencing and the required referencing format, please refer to the ECU Referencing Guide, which can be found from the following URL:

<http://www.ecu.edu.au/centres/library-services/how-to-guides/referencing>




If you do not know how to reference correctly, you can book a session with an ECU librarian (see link above) or take a workshop through the Academic Skills Centre (click on the link in “ECU Support” section in the green menu in our Blackboard site).

Note that in this assignment it is acceptable not to have any references, as long as you do not use any material outside the lecture notes or unit textbook to help you with the assignment.

## ACADEMIC INTEGRITY

The Portfolio assignment is a group assignment. Never give anyone outside your group any part of your assignment – even after the due date or after results have been released. Do not work together with other groups on this assignment – helping someone by explaining a concept or directing them to the relevant resources is fine, but doing the assignment for them or alongside them, or showing them your work, is not appropriate. An unacceptable level of cooperation between students (who belong to different groups) on an assignment is collusion and is deemed an act of academic misconduct.

If you are uncertain about plagiarism, collusion or referencing, you should seek support from your unit coordinator or a Senior Learning Advisor before you submit your assignment. [You should also review the information about academic integrity on the ECU website.](#) Please ensure that you have read and understood the information on plagiarism provided on Blackboard, including the Academic Integrity Module. Repeat offences in other units may result in course termination.

ACADEMIC INTEGRITY TICK-BEFORE-SUBMIT CHECKLIST	
<b>PLAGIARISM</b>  ✓ I have not copy and pasted from external sources without appropriate citation ✓ My in-text and end-text citations follow APA 7 guidelines ✓ I have not used my own or other student's previous assignment work	
<b>COLLUSION</b>  ✓ I have not worked with any other students on this assignment unless permitted ✓ My assignment is not based on or derived from the work of any other students ✓ I have not shown or provided other student(s) with my assignment at any point	
<b>CONTRACT CHEATING</b>  ✓ I have not asked or paid someone to do this assignment for me ✓ I have not used any content from a "study notes" or "tutoring" service / website ✓ I have not had a friend or family member assist me with this assignment	
IF YOU ARE UNSURE ABOUT ANY OF THE ABOVE, DO <u>NOT</u> SUBMIT YOUR ASSIGNMENT BEFORE SPEAKING WITH YOUR UNIT COORDINATOR OR ECU LEARNING ADVISOR	