School of Computing, Electrical & Applied Technology

Course No: HTCS6702	Cryptography	Level: 6 Credits: 15

Student Name:	**Assessor Name:**
Student ID:	**Programme Name: New Zealand Diploma in Cybersecurity**
Assessment Type: Assignment	**Weighting: 70%** **Marks: 100**

Student declaration

I confirm that:

- This is an original assessment and is entirely my own work.
- Where I have used ideas, tables, diagrams, etc., of other writers, I have acknowledged the source in every case.
- This assessment has not previously been submitted as assessed work for any academic course.

Student Signature:	**Date:**

Assessment Summary	Marks Obtained	Resubmission/Resit	
Opportunity 1 Date:	/	Yes/No	
Opportunity 2 Date:	/	Pass/Fail	
Total marks obtained	/ %	**Overall Grade/Result**	

In signing, I can confirm that this assessment has been marked against the marking rubric of this assessment.

Assessors signature: ……. **Date: …….**

Assessment Mapping

After completing this assessment, the student will have met the following learning outcomes related to the graduate profile outcome.

Graduate Profile Outcome	Learning Outcome	Part 1 Task 1	Part 1 Task 2	Part 1 Task 3	Part 1 Task 4	Part 2
Assess, select, plan, implement and validate cybersecurity approaches and controls to support organisational objectives and operations.	2.Analyse the design concepts of data integrity and authentication mechanisms to support organisation's security requirements.	✓	✓		✓	✓
	3.Apply key management and distribution approaches to secure remote services.	✓		✓	✓	✓
Analyse organisational contexts from a security perspective using information management principles and terminology, data inputs, organisational strategy and processes, outputs, systems, and stakeholders' roles and responsibilities.	4. Analyse access models to manage sensitive data access according to an organisation's security requirements.	✓		✓	✓	✓

Assessment instructions:

- This assignment consists of two parts.
- You will work in team of two to complete part 1 and individually to complete part 2 of this assignment.
- Read the scenario provided on **page 4.**
- You will analyse the cryptography mechanisms to manage access to sensitive data of a given organisation. For this your team will need to setup testing platform and validate the security setup.
- For part 1 your analysis should be research based and findings must be presented in form of a written technical document with a count of 3500 word [+/- 10%], excluding reference list, table of contents, presentation task or any other administrative sections (e.g. appendix to explain system configuration and setup).
- For part 2 your individual reflection must be presented with a count of 500 word [+/- 10%].
- Your part 1 technical document must be professional and organised. A recommended format for the report is:
  Title page
  Table of contents
  Introduction
  Part 1 (Task 1, 2 and 3)
  Conclusion
  References
- Correctly reference your used sources in-text and include a full reference list at the end of each part of the portfolio, using APA 7th or IEEE edition guidelines.

Assessment submission instructions:

- Your technical document must be presented in the format stated above and must have margins and page numbers.
- Upload your technical document to the Moodle link "**Upload Team Technical Document here**" (the link will be visible on Moodle page at week 15).
- Upload your reflection document to the Moodle link' **Upload Personal Reflection here**" (the link will be visible on Moodle page at week 15).
- The due date and time for both documents are the **22nd of June, 2022, before 23:00**.

Read the scenario given below carefully

New Zealand's "Phone-me" company provides IP-phone services for end customers over the country. You are part of the cybersecurity team. The company's Chief Technology Officer (CTO) has asked your team to design a System Client to remotely access and update the end-user personal information and add or update the services the end-user subscribe to.

The CTO has briefed your team of Customer Obligations which are:

- No end-user data should be saved on the customer end.
- A two-phase security password should be used.

Part 1: Team work [Total = 85 Marks]

Task 1 **[12 marks]**

- Identify and discuss a minimum of two Business Obligations and two Regulatory Obligations for end-user information security.

Task 2 **[10 marks]**

- Identify and analyse the concepts of data integrity and authentication mechanism(s) for the organisation's Security Requirements.

Some of the organisation's security requirements are specified in the scenario, and some are identified by your team in task 1.

Task 3 **[53 marks]**

You need to design a test platform for your system client, which must include the following:

1. Design a client-server platform that remotely accesses a database stored on the cloud. [5 marks]
2. Create the platform designed in question 1. [5 marks]
3. Identify and apply a symmetric key management algorithm for the encrypted communication between client and server. [7 marks]
4. Identify and use a key distribution approach to manage encryption keys. [10 marks]
5. Identify and analyse two access control models that can be used on your platform according to your organisation's security requirements. [16 marks]
6. Based on your analysis in question 5, apply an appropriate access control model to the system. [10 marks]

Task 4 **[10 marks]**

- Your team will present the findings from tasks 1, 2, and 3.
- Your presentation will be a maximum of 20 minutes long. Both of you will need to present.
- The structure of your presentation needs to include the following: introduction, findings from tasks, and conclusion/summary.
- You will prepare a visual presentation using Microsoft PowerPoint or similar software.
- Your presentation will be recorded for marking and moderation purposes.
- Familiarise yourself with the attached observation checklist to ensure you meet the requirements. Your lecturer will complete the attached observation checklist for each team member.
- The presentation date will be the next day after submission.

Presentation observation

School of Computing, Electrical & Applied Technology

Name of Student:

Name of Observer:

Date of Presentation:

Indicate if the student has met the criteria during the process of achieving the objective. Use the space to add comment for feedback to the student and for moderation purposes.

Criteria	Max Marks	Your mark	Comment
Content: The student demonstrates full knowledge with explanations and elaboration.	3		
Structure: The student presents information in a logical, interesting sequence which audience can follow.	2		
Body language (includes movement and gestures, voice, speed, eye contact, clarity, tone, good rapport with the audience)	2		
Timing The student spoke for a minimum of 5 minutes	1		
Effective use of visual aids	2		
TOTAL	**10**		
Extra Notes:			

Observer's Signature: **Date:**

Part 2: Individual Reflection **[Total = 15 Marks]**

Individually reflect on the design and analysis of the client system and how this is addressing the company's problem.

School of Computing, Electrical & Applied Technology

Marking Scheme

Student Name:

Marking Scheme				
		Maximum Mark	Your Mark	Comment
Part 1	Task 1	12		
Part 1	Task 2	10		
Part 1	Task 3	53		
Part 1	Task 4	10		
Part 2		15		
	Total	**100**		

Marking criteria

	Criteria	Break down of marks	Marks awarded	Comments
Part 1 Task 1 [12 marks]	• Minimum two business obligations are correctly identified and discussed • Minimum two regulatory obligations are correctly identified and discussed	6 6		
Part 1 Task 2 [10 marks]	• Identification of data integrity concept for the problem. • Identified data integrity concept is analysed. • Identification of authentication mechanism(s) concept for the problem • Identified authentication mechanism(s) concepts are analysed.	2 3 2 3		
Task 3 Question 1 [5 marks]	• An interface to access the database and the cloud are designed appropriately	5		
Task 3 Question 2 [5 marks]	• Interface designed in question 1 allows to read and modify the database	5		
Task 3 Question 3 [7 marks]	• Identification of symmetric key management algorithm • Symmetric key management algorithm is setup on the system	2 5		

Task 3 Question 4 [10 marks]	• Identification of an appropriate key distribution approach • The identified key distribution approach is set up on the system.	2 8		
Task 3 Question 5 [16 marks]	• Two access control models are identified • Each access control model identified is analysed. Analyses include a comparison between the two and how they would be used.	2 marks each 6 marks each		
Task 3 Question 6 [10 marks]	• Access control models is applied to the system. The selection of the models is based on the analysis done in question 5. • A test scenario for the access control model is provided.	6 4		
Part 2 [15 marks]	• Reflection demonstrates a clear understanding of system layout and architecture. • Reflection also demonstrates how the system developed is addressing the company's problem	6 9		