SUPERVISOR'S USE ONLY

2

91898

Mana Tohu Mātauranga o Aotearoa
New Zealand Qualifications Authority

Level 2 Digital Technologies and Hangarau Matihiko 2025

91898 Demonstrate understanding of a computer science concept

Credits: Three

Achievement	Achievement with Merit	Achievement with Excellence
Demonstrate understanding of a computer science concept.	Demonstrate in-depth understanding of a computer science concept.	Demonstrate comprehensive understanding of a computer science concept.

There are two questions in this assessment. Choose ONLY ONE question to answer.

You should aim to write **800–1,500 words** in total.

Achievement

TOTAL 03

INSTRUCTIONS

There are two questions in this assessment, on the topics of:

- artificial intelligence (AI) (page 3)
- computer encryption (page 8).

Choose ONLY ONE question to answer. Note that parts (b), (c), and (d) of each question include options for you to choose from.

Read all parts of your chosen question before you begin. Do not repeat your response in different parts of the question.

You are not permitted to access any resources (either in hard copy or online) other than those supplied in the assessment itself.

QUESTION TWO: Computer encryption

(Note: **Do not** answer this question if you have completed Question One.)

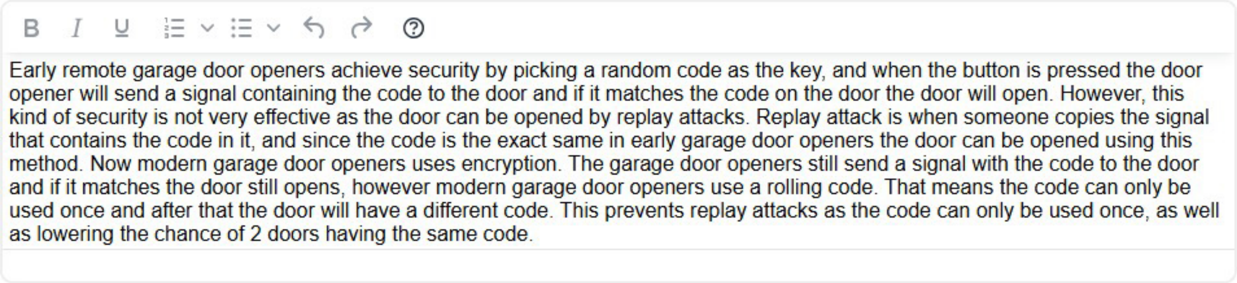
[redacted]

[redacted]

Source (left image): https://www.buiclub.com/info-3543.html
Source (right image): https://cdn.automationdirect.com/static/manuals/d4user/appxh.pdf

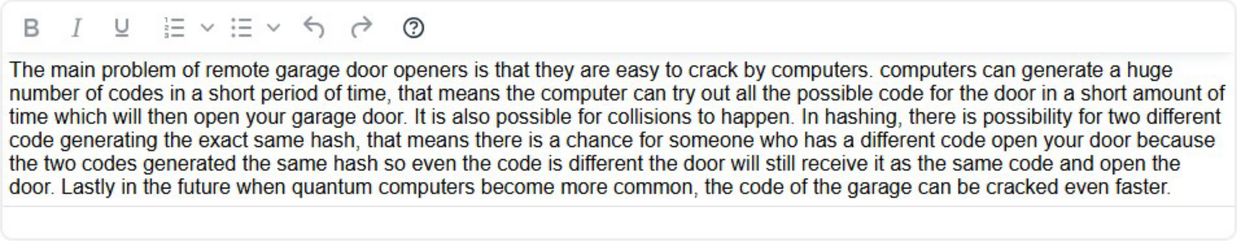
Early garage door openers often had 12 dip (0 or 1) switches as a method of security.

(a) (i) How was security achieved, and how effective was it?
Modern garage door openers use encryption. How is this implemented? Give TWO ways in which they improve security.



Early remote garage door openers achieve security by picking a random code as the key, and when the button is pressed the door opener will send a signal containing the code to the door and if it matches the code on the door the door will open. However, this kind of security is not very effective as the door can be opened by replay attacks. Replay attack is when someone copies the signal that contains the code in it, and since the code is the exact same in early garage door openers the door can be opened using this method. Now modern garage door openers uses encryption. The garage door openers still send a signal with the code to the door and if it matches the door still opens, however modern garage door openers use a rolling code. That means the code can only be used once and after that the door will have a different code. This prevents replay attacks as the code can only be used once, as well as lowering the chance of 2 doors having the same code.

(ii) Identify and explain some of the main problems or issues with remote garage door opener security.
Your answer can include key problems and issues that are current, and/or those that have been resolved.
In your response, ensure that you demonstrate clear links to computer science concepts.



The main problem of remote garage door openers is that they are easy to crack by computers. computers can generate a huge number of codes in a short period of time, that means the computer can try out all the possible code for the door in a short amount of time which will then open your garage door. It is also possible for collisions to happen. In hashing, there is possibility for two different code generating the exact same hash, that means there is a chance for someone who has a different code open your door because the two codes generated the same hash so even the code is different the door will still receive it as the same code and open the door. Lastly in the future when quantum computers become more common, the code of the garage can be cracked even faster.

Source (left image): https://www.encryptionconsulting.com/education-center/what-is-sha
Source (right image): https://simplilearn.com/tutorials/cryptography-tutorial

(b) (i) Explain how ONE of the following is used or implemented, or occurs.

- SHA-256 (Secure Hash Algorithm)

OR

- The key exchange problem.

Enter your selection here: The key exchange problem

Write your answer in the box below.

The key exchange problem is one of the biggest problems of symmetric encryption. In symmetric encryption, the two people communicating will agree on a secret key, then when one person sends a message to the other person he will encrypt the message using the secret key they agreed on and the person receiving the message will decrypt the message using the same key to get the original message the person sent. this is so that if someone intercept the message, they will have no idea what the message is about. The problem is, how could they both agree on the same secret key if they haven't met each other in person. If they just send the key to the other person and the key is intercepted the person intercepting this will know what the key is and now they can decrypt the message between the two people and know what they are talking about. This is known as the key exchange problem. The solution to this is asymmetric encryption, asymmetric encryption work by the two people agree on a number, then they each pick a secret number that they wont tell anyone. then they each combine their secret number with the number they agreed on at the start and send it to the other person, That is known as their public key. They each then combine it with their own secret number which is known as their private key to get a number. If the math is done correctly the number they each get after combining with their private key will be exactly the same, which means they have now got a key that can be used to encrypt their message using symmetric encryption. This solves the key exchange problem because even if the person intercepting the messages get the public key, they wont be able to decrypt the message as they don't know the private key.

(ii) Choose ONE of the following to answer:

- Explain how encryption has been used in healthcare to address a need.

OR

- What opportunity has encryption provided in healthcare?

Enter your selection here: Explain how encryption has been used in healthcare to address a need.

Write your answer in the box below.

Encryption is used in healthcare because all of the patient's data will be stored in the hospital's data bank. So if the data is not encrypted and the database gets hacked, the hacker would've gotten all of the patients' data. That's why we need encryption in healthcare so that even if the database gets hacked, the hacker will only get the encrypted data and will have no way of decrypting the data and getting the patients' information. This prevents others, such as the government or companies such as the insurance company to get the information of the patient, so that the companies can't promote their product to them as well as the government can't use that to gain control over the patient

(c) Choose ONE of the following to answer:

- Explain, giving examples, what can be done to future-proof AES (Advanced Encryption Standard).

OR

- Explain, giving examples, known ethical issues in privacy with encryption.

Enter your selection in the box below:

Explain, giving examples, known ethical issues in privacy with encryption.

Write your answer in the box below.

Encryption is important for our everyday lives as we access the internet so often. It unlocks a lot more opportunities, such as online banking. Without encryption, it is never safe to type our bank details online. Encryption also allows people to communicate online without having to worry about someone else intercepting the message. However, criminals can also use encryption to communicate online without having to worry about the police listening in. If there is a "backdoor" for the police to decrypt messages, the criminals will not communicate online, making it harder for them to plan a crime and also making it easier for the police to stop a crime before it happens. The problem is, if that "backdoor" existed, other citizens' messages could also be decrypted. That means, even if someone who was not planning to commit a crime sends a message as a "joke" to his friends, this could lead to them getting arrested even if they didn't plan on committing a crime. The government having a method of decrypting the message could also mean that they can gain more control over their citizens, as they can tell everything their citizens are doing online. Another issue is. If a patient is going to a hospital, their encrypted data will be saved in the hospital's database. Encrypted messages can only be decrypted using the key. But the problem is, who should have the key? If the government has the key, they might use it against the patient. If the doctor has the key, what if the doctor shares the key with someone else? If the patient has the key, what if they needed help but they couldn't give the doctor the key? Then the doctor might identify the issues incorrectly and could possibly lead to the patient not getting the proper treatments. That's why the doctors should hold onto the key so if the patient needed help the doctor can access the patient's data and get a better understanding of the situation.

Achievement

Subject: Level 2 Digital Technologies

Standard: 91898

Overall grade: 03

Q	Part		Marker commentary
Two	(a)	(i)	A satisfactory answer was given. The candidate discussed codes in the remote and opener, replay attacks, and encryption. There was, however, a lack of detail in some aspects.
		(ii)	This answer helped to expand on the response to (a)(i), reaching Achievement level for this part. It lacked sufficient depth for Merit.
	(b)	(i)	A good, detailed answer was given to this question, covering the key exchange problem and how public / private encryption works.
		(ii)	The response to this question lacked detail and specificity to the healthcare area.
	(c)		The answer discussed the need for encryption in general, and then the issues that law enforcement have with criminals using encryption.
			Overall, this response was at Achievement level. To gain a higher grade, the candidate would have needed to fully answer question (a) and provide a more detailed answer to question (b)(ii).