2

NZQA
NEW ZEALAND QUALIFICATIONS AUTHORITY
MANA TOHU MĀTAURANGA O AOTEAROA

QUALIFY FOR THE FUTURE WORLD
KIA NOHO TAKATŪ KI TŌ ĀMUA AO!

COMMON ASSESSMENT TASK

Level 2 Digital Technologies and Hangarau Matihiko 2020

91898 Demonstrate understanding of a computer science concept

Credits: Three

Achievement Criteria		
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.

Type your School Code and 9-digit National Student Number (NSN) into the header at the top of this page. (If your NSN has 10 digits, omit the leading zero.)

Answer all parts of the assessment task in this document.

Your answer should be presented in 12pt Arial font, within the expanding text boxes, and may only include information you produce during this examination session.

You should aim to write between **800–1500 words** in total.

Save your finished work as a PDF file with the file name used in the header at the top of this page ("SchoolCode-YourNSN-91898.pdf").

By saving your work at the end of the examination, you are declaring that this work is your own. NZQA may sample your work to ensure that this is the case.

You must not access the Internet or use any printed or other resources except for this assessment.

Merit

05

SchoolCode-YourNSN-91898.pdf

INSTRUCTIONS

Read all parts of the assessment task before you begin.

Select ONE of the following computer science concepts:

- error control
- encryption
- artificial intelligence.

Type your chosen computer science concept in the space below:

Encryption

Begin your answers on page 3.

SchoolCode-YourNSN-91898.pdf

ASSESSMENT TASK

(a) Describe at least two examples in which your chosen computer science concept is either **used**, **implemented** or **occurs** in current digital technologies.

The most common use of Encryption is to store passwords, let's say in a scenario where your password has been breached online, anybody can use that password to login as you, view your information and steal it too. The solution to this is the use of one-way encryption. In a one-way encryption system, the data can only be encrypted and not decrypted because it is not a two-way encryption system that has public and private keys in it. An example of a one-way encryption system is hashing. Hashing is a process where your password is stored as a random string on the site you are on and every time you log in, the hash is then compared with the password you type in, if successful then it will allow to enter. A salt is a random string that is added to your hash to make it different from everyone else's just in case you were to have the same password as someone else. A pepper is a character that is added to the hash which completely changes it. This is good because If someone is to breach the site and attempt to steal your password, they would only see the hash that is stored on the site and not your actual password. This is a great solution to people breaching sites and steal people's private data.

Another example of encryption which is a basic one is the use of emailing. When you email someone, your data which is in plaintext is decrypted into scrambled text and once it reaches the receiver it is decrypted back into plaintext again. This means that if someone were to breach the connection between the user and the receiver, they would just see scrambled text, this encryption system is called a two-way encryption system which usually involves a public and private key. The public key will be used to encrypt data and the private key will be used to decrypt the data that was encrypted by the public key. This is really great as it ensures safety of people's data. It shows that something so big and useful as encryption Is used for something so small like email which is just a normal day to day task.

(b) **Opportunities** include providing a solution, improving functionality and solving a known issue / risk.

Select ONE of the following two options:

- How **is** your chosen computer science concept **currently** applied to address an opportunity?
- How **could** your chosen computer science concept be applied to address an opportunity?

Copy and paste your chosen option in the space below:

How **is** your chosen computer science concept **currently** applied to address an opportunity?

Answer the question about your selected option in the space below:

Encryption is used on a day to day basis to ensure the safety of people's private data to keep away from those with malicious intent. An example of this would be the Encryption involved in the use of medical records. When you go to hospital, the doctors can easily access your medical data on their database provided that you are registered there. And if they want to transfer you to another hospital, the doctors in the other hospital can access your medical records as well. This is done safely with two-way encryption, where both hospitals would contain a public and private key to encrypt and decrypt the data. A one-way encryption system would also be involved for hospital staff logins. This is to be extra safe and to ensure that only the authorized staff can access something important like your private medical data. Hospitals do this because patients expect their doctors to keep their private medical records private, so it is simply ethical to keep their records encrypted to prevent many crimes. An example of a crime that can happen in this situation is identity theft, where someone can access your medical data and possibly get their hands on your ID as well. They can go as you to the hospital and possibly get their hands onto some drugs in the hospital. The great thing about encryption is that it is used to ensure that it kept away from those with malicious intent and is readily available for those who need it to help us.

(c) **Mechanisms**

(i) Explain the use of an **algorithm** or **technique** used in your chosen computer science concept.

For example, you could explain:

- how the Luhn algorithm works
- the purpose of private / public keys or password hashing
- why an artificial intelligence might be considered as intelligent.

Algorithms relate to encryption because that is what encryption basically is, from a basic standpoint, you have your data which is in plaintext, then that data is then put through an algorithm and the result is your encrypted data. For a two-way encryption system, you would then need to put the encrypted text back through an algorithm to make it plaintext again. An example of an algorithm is the RSA algorithm which involves both a public and private key, the public key is given to anyone who needs it to encrypt and the private key is kept secret for someone to decrypt the data. The good thing is that the data can only be decrypted using the private key so if an attacker were to get their hands on private information they would not be able to decrypt it without the private key, and the public key won't work because that is used for encrypting data and not decrypting.

The process works by multiplying two very large prime numbers that are 100+ digits, the third number which is the result, it becomes the public key. Finding factors of the third number is almost impossible and would take excessively long to factorize. But if you have the third number (public key) and one factor then finding the other factor would be quite easy. For example if I told you to factorize the number 96,709 it would take you a good while to factorize, but If I told you to factorize 96,709 and told you that one of the factors is 997, then you can easily divide and find the other answer which 97.

This is the really great thing about this algorithm, that it first of all it uses prime number which can only be divisible by 1 and itself and that it consists of 100+ digits which means that there is no fast way or shortcuts or even fast algorithms that can factorize the public key. Making this a really great algorithm to use.

(ii) Explain the **protocol** or **procedure** used in your chosen computer science concept.

For example, you could explain:

- how an organisation ensures the protection of data by using encryption
- how barcodes are used, and errors identified
- how an artificial intelligence system is used to achieve a purpose.

Protocols are designed to ensure that sites are completely safe to use because if your site contains private data then you should be using encryption to ensure as much safety as possible. An example of a protocol is Hypertext Transfer Protocol Secure or most commonly known as HTTPS. HTTPS is used to transfer data over the World Wide Web (WWW) and to prevent attackers from intercepting and changing the communication between your browser and the server.

Requests and Responses between your browser and the server are encrypted using something called Transfer Layer security. The site uses a two-way encryption system that uses public and private keys, the private is kept secure on the site and the public key is given to anyone interacting with the site. This is to ensure that if anyone were to intercept the communication and breach the site, they would only see random characters and not something very important like credit card details.

Protocols are something very essential on the internet and should be used alongside encryption systems to ensure the maximum security of people's private data.

(d) **Impacts**

Select ONE of the following impacts:

- Ethical issues
- Human factors.

Copy and paste your chosen impact in the space below:

Human Factors

Explain how this impact relates to your chosen computer science concept.

Because of us humans, we have created something so great and useful as encryption to help us in our daily lives and to ensure the safety of our private data. But the problem is that humans are the main source of cybersecurity attacks. Encryption cannot solve the problem of people falling prey to phishing attacks and being manipulated into spilling their private information.

The very big human factor is that people use too much simple passwords which means that breaking methods such as rainbow tables, brute force attacks become easy to use. And these problems can be solved by using password managers or two-step authentications to ensure more safety.

The human factor is that us humans are destroying/attacking the very thing we made.

(e) Comprehensively explain the key problems or issues related to your chosen computer science concept.
This can include showing links between and expanding on your answers to parts (a)–(d).

The biggest problems in today's encryption world are the rise of quantum computers and human errors. In the current day thanks to complex algorithmic encryption systems, attackers can only access your private data as they have time and money. But with quantum computing arising, people will be able to compare more hashes per second with a fraction of the price, it will become super easy to breach passwords.

To combat the progression of technology, we have to make more complex algorithms but no matter how complex our algorithms get, attackers are always one step behind and if quantum computers full develop and is in the hands of an attacker, all of the computer algorithms will available to them and they will have the ability to do things that normal computers cannot do. So, it is our job to future proof this and fight against quantum computing to keep encryption in safe hands.

Encryption is only as good as it's user because you can have all the encryption in the world but if you give someone your password, then encryption becomes useless. The good thing here is that a site stores the hashed version of your password so you could easily just change your password through your email, but the bad thing is that the site cannot know if an attacker is signing in as you. All it needs to do is compare the hash and if it is successful, they're in. Another problem is that people use the same password for all of their sites, so If someone were to breach your password, they would be able to access all of your sites instead of one, causing some major damage.

Not all attacks are via computer though, a lot of phishing attacks occur via phone, where you would get a call saying that your computer is broken and that you need to give your password to fix it. What they do instead is steal your username and password, view your information and steal it too. Some of these attacks are obvious whereas some are not.

The human factor is that people use very simple and common passwords which means that that password will most likely be on a rainbow table with it's given hash. So with a blink of an eye and all of your stuff is gone.

These human errors make encryption totally useless and can be avoided quite easily with solutions such as using different passwords for each site, using difficult to guess passwords and changing your passwords regularly.

It is crucial that we as users of technology become smart to these tricks, learn what to trust and what not to trust because encryption becomes useless if we do not take better safety precautions ourselves, encryption isn't fool proof.

Merit Exemplar 2020

Subject	Digital Technologies	Standard	91898	Total score	05

	Grade score	Annotation
	M5	*Computer science concept: Encryption* In part (a), the candidate gave two detailed examples of where encryption can be found. In part (b) the opportunity where hospitals use encryption was given, along with good detail, without repetition from part (a). In part (c) both answers covered different areas, demonstrating clear understanding of the mechanisms. In part (d) more detail and depth was required to demonstrate understanding of the impact of encryption. Part (e) included a number of good responses. On balance, parts (d) and (e), along with the standard of the previous parts, provided sufficient evidence for the award of a Merit grade.