2

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 2021

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.

Type your School Code and 9-digit National Student Number (NSN) into the space below. (If your NSN has 10 digits, omit the leading zero.) It should look like "123-123456789-91898".

There are three questions in this document. **Choose ONE question to answer.**

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

Your answers should be presented in 12pt Times New Roman font, within the expanding text boxes, and may include only information you produce during this assessment session. Internet access is not permitted.

Save your finished work as a PDF file as instructed by your teacher.

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 this is the case.

Merit

TOTAL 05

ASSESSOR'S USE ONLY

INSTRUCTIONS

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

- Computer security (page 3)
- Encryption (page 8)
- Error control (page 13).

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

Read all parts of your chosen question before you begin.

OR: **QUESTION TWO: Encryption**

(a) (i) Name a **specific** New Zealand-based company or organisation that uses encryption.
Note: If you want to discuss your school, state "My school".

Edge (School attendance and student record website)

(ii) Give at least TWO examples of ways encryption is used by this organisation.

Encryption is used by edge in a few ways, firstly we have hashing. Edge uses hashing to insure that the person trying to access it is either a student, a parent or a teacher, they use hashing to encrypt their password to store on their database, and to compare to the password hash with when they next login.

Secondly edge uses encryption for all communications between the server and the client devices communicating with them. This makes all communications private, and unreadable by people not intended to read the content.

(iii) What do these uses of encryption enable this organisation to do that would otherwise be difficult or impossible?

Edge keeps medical information of students, NCEA grades, contact information of students and care givers, attendance records, incident. These sorts of things are something that must be kept private. if there was no encryption ensuring that who was logging on wanting to use the service, then a student could go in change grades, attendance and other things that the school would want to keep an accurate record of. Without encryption a service like edge would not be able to exist as the risk of information getting into the hands of somebody how has ill intentions.

Because Edge is used for attendance records, it becomes a security concern, as it is important the school and parents know where a child is at all times (during school time). If somebody were to be able to change attendance records, this would be a problem as the attendance records would be inaccurate, and the student could be elsewhere from what's stated on this Edge. And without encryption it would be easy for a student to be able to change information like that.

It also becomes an educational concern without encryption, as Edge reports student grades to NZQA, without encryption it would allow students to be able to change their grades and get higher marks then they are capable of.

The ability for Edge to be used across the country would also not be viable without encryption which is a very important part about edge, you could be on a ski trip with school and if anything happened to you the teacher could find out any medical conditions you have and be able to contact your parents and let them know what's going on.

(b) Choose TWO of the following to answer:

- How do private and public keys work in public-key encryption?
- What are the concerns if a website user clicks on “I forgot my password” and the website emails them their original password?
- What different encryption procedures can an organisation use to ensure the security of its customers’ accounts?

Choice (1) – (copy and paste below)

What are the concerns if a website user clicks on “I forgot my password” and the website emails them their original password?

Response

The concern that is raised when you click “I forgot my password” and shown you original password is the security of your password. A website being able to do something like this means one of two things, either your password was stored in plain text, or the encryption they used to store your password was so poor they were able to reverse the encryption with their computers. What’s wrong with a password being stored in plain text? This means that if an attacker were to get into the database for user logins they would be able to see every single user and their corresponding password, this is an issue as the attacker could start logging into the service as a user and steal the user’s information, there would be no way for the system to know whether it was an attacker using the password, or the user without using a second form of verification. And because people tend to have the same passwords across many sites and services the attacker could go on to other sites and steal even more information. If it’s encrypted in the first place then what’s the problem? The issue is that the aim of encryption is that it should be so hard to find out the contents of the encrypted password that it would take lots of computing power and time, costing whoever it was trying to find the contents a lot of money. It also stops administrators of the site from seeing your password. if a site were to simply just decrypt your password this means that anyone working for the company if they had access to where the encrypted passwords were stored, they would be able to find the password of anyone they wanted, attackers could do the same. This is why it is important for companies to keep their encryption up to date, to make the task of finding encrypted information cost whoever wanted to find it lots of time and money, making it often not viable.

Choice (2) – (copy and paste below)

How do private and public keys work in public-key encryption?

Response

Public and private keys solve the complicated issue of get information to somebody over the internet securely with only ever using the internet. If you for example wanted to securely message to your friend from another country, and the only way to do so was over the internet, you couldn't send them a key to a normal two-way encryption as somebody could intercept that key without anyone knowing and then reading all the messages transmitted.

A way to solve this is to use a public and private key encryption. How they work is anyone can have the public key, and it is only used to encrypt whatever information you wish to be encrypted. And viewed by the person intended to receive that information. Information that is encrypted by the public key is not able to be decrypted by the public key, it can only be decrypted by the private key. The private key is kept by the receiver of the information and is to be kept private, as it is the only way to decrypt information encrypted by the public key. This method of encryption uses big prime numbers and the sum of those big prime numbers multiplied together, it is almost impossible to find the prime numbers that went into making the sum, but it you have a key which is one of those prime numbers the calculation to decrypt becomes very easy.

So if we were able to put this in our example, I would send my friend the public key, with which they could then encrypt with my public key and send me a key for a simpler, and faster two-way encryption and I would be the only recipient of that key as I was the only one with the private key in order to decrypt it.

(c) Choose ONE of the following to answer:

- What are some ways that encryption can be future-proofed?
- What are some ways that human factors influence decisions about encryption?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

What are some ways that human factors influence decisions about encryption?

Response

A good example is this is hashing. Sites use hashing algorithms to store passwords, and if they keep their systems up to date, they should also use Salt, Pepper, and cost.

Salt is stored as plain text on the database. Salt is a user unique string that gets added to the end of a password for example user 1 may have the password “12345” and a Salt of “WZ” and user 2 may also have the same password but their Salt is “BH” before both user’s passwords are put through the algorithm the password and Salt are combined, so user 1’s would become “12345WZ” and user 2’s becoming “12345BH”. This means that even when the user’s passwords are the same, the hash values are different. This is a grossly simplified version, Salts will be 10s or 100s long values.

Pepper is kept secret by the site. Pepper is a site unique string that gets added to the start of a user’s password and cost is how many times a password and its hash is run through the algorithm. So let’s take user 1’s password. company A’s Pepper is “JJ” and company B’s Pepper is “RE”. User 1’s password on both sites with the Pepper added would be “JJ12345” for company A and “RE12345” for company B, this shows that even if a user were to have the same password among other sites, this wouldn’t be provable unless you were to try login as the user and after too many tries the system would lock you out.

Why do we need Salt and Pepper? Humans are very simple, passwords are often the weak point to encryption as humans don’t like to choose very strong, or unique passwords. The issue with this is that multiple users can have the same password in fact it’s so common for this to happen there is something called a rainbow table, a rainbow table is when an attacker finds the hashes for the most common passwords for people to use, for example they will figure the hash for “12345” or “password” and then see if anyone’s hash is the same as their hash and they know that the user used that if the hashes match. Salt and Pepper makes the users passwords unique from site to site and from other users no matter what.

(d) Choose ONE of the following to answer:

- A person is using public Wi-Fi in a café. They plan to set up a new social media account and then log in to it. Explain how the encryption process works, including any key problems or issues.
- Assuming usable quantum computers become a reality, what problems is this likely to cause with data that has already been encrypted, and with data that needs to be newly encrypted. (It may help to create a possible timeline showing quantum computers becoming available to different organisations and individuals.)

If relevant, you should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

Assuming usable quantum computers become a reality, what problems is this likely to cause with data that has already been encrypted, and with data that needs to be newly encrypted. (It may help to create a possible timeline showing quantum computers becoming available to different organizations and individuals.)

Response

Quantum computers are much faster than the computers we use today. With the constant rise in technology's capabilities encryption algorithms always have to be a step ahead, quantum computers are able to solve complicated encryption algorithms we use today in a fraction of the time we take to do the same today. The issue if quantum computers becoming a reality is that we would need to upgrade all of our encryption algorithms, the issue with doing so is that we can't decrypt all of the currently encrypted data without privacy being a concern, as user's data would become unencrypted for a period of time, this means that while it is unencrypted somebody could view the contents and breach that user's privacy. In order for a switch over to quantum encryption would be to restrict the sale of quantum computers until people switched their data to being encrypted so that it would almost impossible for a quantum computer to be able to find the contents. No matter what, data would always have to be unencrypted to make this change so there's always risk of somebody getting a hold of the unencrypted data. Quantum computers should slowly be released to trusted companies who would work towards finding quantum encryption algorithms, and work towards a safe way to be able to make the switch.

Merit Exemplar 2021

Subject	Level 2 Digital Technologies	Standard	91898	Total score	05

Q	Grade score	Annotation
2	M5	The candidate has given two different examples of the way encryption is used by an organisation. In part (b), the candidate has given a good explanation of the implications of a website emailing someone their original password, and the risks of storing unsecured passwords. The explanation of public-private key encryption demonstrates a good level of understanding of the concepts involved. In part (c), the candidate explains well how users are a security weak point when choosing and reusing password, and how providers can mitigate this issue. In part (d), the candidate has not demonstrated sufficient understanding of the way that quantum computers becoming a reality would pose a risk to most current encryption methods.