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, 2019

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 HAND THIS BOOKLET TO THE SUPERVISOR AT THE END OF THE EXAMINATION.

Excellence
07

INSTRUCTIONS

Read all parts of the assessment task before you begin.

Select ONE of the following computer science concepts:

- computer security
- encryption
- error control
- complexity and tractability
- artificial intelligence.

Type your chosen computer science concept in the space below:

Encryption

Begin your answers on page 3.

ASSESSMENT TASK

(a) Briefly explain your chosen computer science concept.

Encryption is the use of algorithms to encrypt data so that it is unreadable and then decrypt it so that it becomes readable again. This is useful when you want to send someone an email and don't want others online to be able to see what you are sending. You encrypt the email and send it so that while it is being sent others just see the encryption and not what the email actually says. Then when it reaches its destination it can be decrypted with a key and read.
Encryption is made up of:
One-way encryption- encryption that cannot be decrypted
Two-way encryption- encryption that can be decrypted with a key
Public private keys- public keys can encrypt but only the private key can decrypt
Backdoors- are ways around encryption or master keys/passwords that are built into a program. You don't know they are there as they are unseen.
Secure passwords- is part of the human side of encryption as you need to pick a sensible password that can't be identified by rainbow tables.
Rainbow tables, hacking, brute force- are a few examples of how to break encryption. Rainbow tables are lists of common passwords and their encrypted hashes, brute force attacks are trying every possible password.
Salting, pepper and cost- salt is a string added after hashing to ensure everyone's hash is different, pepper is a character added before hashing that will completely change the hash and cost is how many times the hashing algorithm hashes.
DRM- encrypted music and video needing a key to play to stop piracy.
SSL- secure socket layer certificate given to secure sites padlock icon insures that transactions are encrypted.
People are fallible- Phishing, they just tell others their passwords and give away info.

(b) Choose ONE of the following three options to answer.

EITHER: **OPTION ONE**
Give details of how your chosen computer science concept is used in current digital technologies.

Encryption is used to keep our private information safe. We encrypt information so that it can't be accessed by others with malicious intent. One example of encryption is medical records. Medical records are encrypted using two-way encryption and kept online so they can be accessed by any hospital that you visit as they will need to know any medical conditions you have. The hospitals are all given the key to decrypt this information as they need it but other joeblogs aren't given a key to decrypt your medical information as they do not need to know. This ensures that your private medical information is kept safe from those that may use it with malicious intent but is readily available to those who need it to help you. Encryption is used to keep information safe and hidden from those who you don't want to have it and gives us reassurance of digital security as we know our information is safe.

OR**: OPTION TWO**
Give details of how your chosen computer science concept is implemented in current digital technologies.

OR**: OPTION THREE**
Give details of how your chosen computer science concept occurs in current digital technologies.

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

Answer ONE of the following two options:

***EITHER*: OPTION ONE**
How **is** your chosen computer science concept **currently** applied to address an opportunity?

Encryption is currently applied to storing passwords. If a site stored your actual password and it was breached, then anyone can see your password and use it. This allows them to log on as you and access all of your information. There is a solution to this provided by encryption in the form of one-way encryption. One-way encryption means that once something has been encrypted it cannot be decrypted economically so no one bothers. A form of one-way encryption that is used to solve the risk of others finding your password is hashing. Hashing is turning your imputed password into a unique string that is always the same when you input the same password. When you input your password into a website to log on the password is hashed and then the hash is stored on the website. Then when you log on again it compares the hash of the password you input to your original hash and if they match your password must be correct. This means that when others breach the website and steal all of its data they can only see your hash and not your password as only the hashes and not the passwords are stored. Because hashing is one-way encryption they can't decrypt the hash to find your password and therefore can't log on as you and steal your information. Hashing is the solution to people with malicious intent wanting your information and is currently applied to address the opportunity of password security ensuring that your information is safe.

***OR*: OPTION TWO**
How **could** your chosen computer science concept **be** applied to address an opportunity?

(d) **Mechanisms**

Select TWO of the following seven mechanisms:

- techniques
- algorithms
- principles
- protocols
- systems
- procedures
- processes.

(i) Type ONE of your two selected mechanisms in the space below:

Algorithms

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

Algorithms relate to encryption because algorithms are all encryption is. To encrypt and decrypt data we use specific algorithms. You start with your data and then you put the data through an algorithm and the resultant is the encrypted data. For two-way encryption you can then put the data back through the algorithm or use a key to decrypt the data back into its original form. An example of an algorithm is the SHA hashing algorithm. The SHA algorithm is a one-way algorithm used to encrypt data that you don't want anyone to be able to find out what it was. The SHA algorithm has many different versions with different levels of security, SHA-1 being the oldest is the least secure as you can decrypt it using your phone in a few seconds. SHA-256 and other higher number SHA versions would take the same phone (that can decrypt the SHA-1 in a few seconds) billions of years. Hashing is a one-way algorithm so the algorithm can't be reversed meaning that to find a password you have to use a brute force attack and try every possible password until you find the one with the same hash. As technology is progressing so is the complexity of the algorithms and as the algorithms get more complex they can give a wider range of outputs meaning brute force attacks take longer. Encrypting algorithms that were thought to be super secure ten years ago not even being used today as they are not secure in today's standards because they do not have a wide range of outputs. The key to good encryption is to have the most up to date and complex algorithms possible. Good algorithms are the algorithms that are the most complex and those with the most outputs. As good hashing algorithms can have millions of possible outputs so finding someone's password is very time consuming and uses heaps of computing power deterring those with malicious intent as it is not worth the time and money. Encryption is basically algorithms with good encryption being good algorithms and bad encryption being bad or old algorithms.

(ii) Type your OTHER selected mechanism in the space below:

Protocols

Explain how this second mechanism relates to your chosen computer science concept.

Protocols are followed by sites to ensure that they are safe and trustworthy. Any site that uses any information should be encrypting the information that it stores so that those with malicious intent cannot gat that information. An example of this is SSL. SSL stands for Secure Socket Layer and is assurance to the user that a website is safe and encrypted. For a website to be able to claim they are secure they will need to acquire a SSL certificate which can be purchased from a SSL certificate provider once they thoroughly check that the site is secure. Sites with SSL will have the little padlock icon to show they are secure and will follow the SSL protocols. Examples of sites that have SSL are online trading sites. For online trading sites you will be needing to put in your bank account details to purchase items. If the site does not follow protocols and have an SSL certificate anyone could be seeing your bank account details and will now have access to your bank account. But sites with SSL have a secure connection with only you and them being able to see your bank account details allowing for secure encrypted transactions giving you assurance that no one can access your bank account. A SSL is usually two-way encryption with the site sending you the public key to encrypt your bank account details and only them having the private key to decrypt the information. Protocols in encryption are essential for maximum security and it is important that they are followed to ensure that information is properly encrypted and not available for those who you don't want to have it.

(e) Explain in depth the impact that ONE or TWO of the following factors has on your chosen computer science concept.

Ethical issues: There is an ethical debate whether encryption is to secure and that it needs to be more transparent as encryption means that no one can access your data and that includes law enforcement agencies. Because of this there are many illegal transactions and things happening online that the law enforcement agencies do not have access to as they are encrypted. This means that the police are one step behind the smart criminals just like hackers are one step behind those who use good encryption. Terrorists can plan attacks online with the information being just there but out of reach as it is encrypted. This has raised ethical issues as people think that the police should have access to this kind of information but if they do have access where do you draw the line and what do they have access to and what do they not have access to.

Social impact: Encryption socially impacts its users by giving us assurance that our information is safe and inaccessible to others. Because of encryption we can be assured that our online transactions and any secrets we may have are safe and kept secret. It allows for businesses to supply clients worldwide without the risk of their information being stolen and everyday people to connect with one another all around the world. This has socially impacted all the users as they now know and do more online because it is a safe encrypted place. Being in New Zealand we do not have everything readily available so we have to buy things from overseas. Without encryption ensuring that these transactions were safe we would not have access to all to the things that we do not have around us. The social impact of encryption most people take for granted as we do not realize without it what life would be like. Imagine the world with no internet, all of the schools and businesses and individuals would have to use paper mail to contact each other and buying something would take weeks as you would have to pack all or the money into a box and send it away before the item is sent to you and then you don't have the assurance the item will even turn up and your money is going to the right place. Having to read through heaps of encyclopedia to find what you can find on the internet in seconds. Of course the internet is not encryption but the internet would not be safe without encryption so no one would use it. Encryption is an essential part of our everyday lives with most people relying on it. For this reason encryption has a huge social impact.

Sustainability:

Human factors:

Future proofing:

(f) 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)–(e).

The key problems of encryption are the possibility of quantum computing in the future and human user errors.

At the moment those with malicious intent can only obtain as much of your private information as they have time and money. But with quantum computing they will be able to compare more hashes per second and it will only cost a fraction of the price meaning finding your password and information will become heaps easier. To combat the progression of technology encryption algorithms have become more complex but no matter how complex they become hackers are just one step behind. But with quantum computing all of the complex algorithms and impenetrable encryption will become easily accessible to hackers so when quantum computing comes with it a new tier of algorithms must be invented to keep encryption secure.

Encryption is only as good as its user because you can have all the encryption in the world but if you tell someone your password then they will be able to access your data. People are fallible and we are prone to phishing attacks in which those with malicious intent instead of trying to break the encryption to find our password as it is too hard just ask us to give them our password. Examples of this are pop up adds that ask you to log on to your email but instead they just take your username and password and do what they want. Because sites store hashes instead of passwords you can change your password through your email as the site doesn't actually know what it is meaning once someone has access to your email they have access to most of the other site you use. Not all attacks are via the computer as well you can receive phone calls saying that your computer is broken and you need to give them your passwords. Some of these scams are obvious and others look legitimate fooling a wide range of people. The human factor of encryption is also peoples password choice because if your password is password or 12345 it will probably be on rainbow tables. Rainbow tables are lists of common passwords and their hashes so if your password is one of these common passwords hackers will quickly identify it and have access to your information. It is important that we as users of technology become smart to these tricks and learn what to trust and what not to trust otherwise encryption is useless and has no point because they can just ask us for our passwords so why encrypt them in the first place. Another part of human error is that we use the same password for multiple sites and we do not change our passwords regularly. It takes time for hackers to find your password via brute force attacks so if you change your password then by the time that they find your password it is something different so they have to start the process all over again. But because people don't change their passwords regularly if at all, passwords are found and people have their information stolen. People also use the same password for everything meaning that if one site that you use does not have up to standard encryption and your password is found then others can use that password to log on to all of the other websites that you use that password for. This makes encryption useless and that one site without dated encryption the weak link in the chain of your information's security. You can avoid this by using different passwords for everything and changing your passwords regularly.

Excellence Exemplar 2019

Subject	Digital Technologies	Standard	91898	Overall grade	07

Q	Grade	Annotation
		The candidate gave a brief explanation of the computer science concept, with a good introduction to a number of topics in the area encryption. In the section dealing with Opportunities, the candidate detailed how one-way encryption for passwords worked, touching on the matter of limitations. This answer would have benefitted from being tied to a specific scenario. In the Mechanisms discussion, the SHA algorithm was explained, again with reference to limitations. The answers for protocols were distinctly different from those for algorithms. This demonstrated the candidate's understanding. The section dealing with Impacts provided answers to two possible impacts. This was a good choice for the candidate. The ethical issues answer was good, but not sufficient for an Excellence grade. The answer to the Social Impact was detailed and provided an answer that was different to that provided to other questions. It did a good job of explain the benefits of encryption. As regards the Key Problems and Issues answer, the candidate took a different approach, looking at encryption. They looked at potential threats to encryption due to quantum computing and human factors.