PROGRESS OUTCOME 7

Looking at cybersecurity

Context

Hamiora has been investigating the concept of encryption and its impact on society. He has learnt that encryption is an important aspect of computer science as it impacts upon all our online activities, including online shopping, banking and financial transactions.

Insight 1: The concept of encryption

Most people take cybersecurity for granted, yet few understand exactly how encryption works. I discovered that encryption is the conversion of data into a form that is unreadable to anyone except the intended recipients. This is important in our society because we all have private information that we don't want the world to see. This includes the things we expect to remain private, like our online searches and the messages we send our friends, but also the things we expect to remain secure, like our banking information when we use internet banking or the credentials for our Wi-Fi networks. Unfortunately, there are malicious people who break into individuals' systems for personal gain. Encryption helps protect against this.

Insight 2: An example of encryption

A simple example of encryption is an XOR cipher used on text, which is stored as binary using the ASCII encoding standard. This relies on a constant binary 'key' that is applied to the input. For simplicity, the binary key is exactly 8 bits long (the length of a byte).

The example below uses the string "Testing testing" (but in binary) as the input and the binary 00010111 as the key.

Input string:	Testing testing
Key:	00010111
Output of XOR cipher (gibberish):	Crdc~yp7crdc~yp

The XOR cipher works by applying the XOR binary operator to each bit of each byte. The binary operator takes two bits and returns true (represented as 1) if the two inputs are different, or false (represented as 0) if the two inputs are the same. One of the two bits is from the key, while the other is from the input string.

Insight 3: Key problems and issues

A major problem with using an XOR cipher on text it that it becomes vulnerable to frequency analysis. This is a technique that uses the known frequency of each letter in a language to guess which letter corresponds to each encrypted character. For example, since letters like e and t are far more common than z and q in the English language, it's highly probable that two of the characters that appear most commonly in an encrypted message are e or t. Using this information, a hacker can guess the code and decrypt the message, thus "cracking" the cipher.

Insight 4: The key distribution problem

Two forms of encryption ensure that only the intended recipient can read a message: symmetric cryptography and asymmetric cryptography. Symmetric cryptography relies on the sender and receiver sharing or exchanging a key securely. Most real-world systems use asymmetric cryptography, or public-key cryptography, which uses two keys instead of one. The first key (the "public key") encrypts a message and can be shared widely. The other key (the private key") decrypts the message and is only known to the recipient of the message.

With symmetric cryptography, the one key must be kept absolutely secret between the two parties. However, in asymmetric cryptography the public key used to encrypt messages can be shared widely without fear of it being used to decrypt messages, because decryption requires the private key.

Insight 5: How asymmetric cryptography is used

A popular form of asymmetric cryptography is RSA (named after its inventors: Rivest, Shamir and Adleman), which uses a public key and a private key. RSA is used on the internet to securely establish a connection between computers and websites. As RSA uses asymmetric cryptography, the website and the computer can send their public keys to each other, without having to worry about communicating secretly.

RSA encryption is used in many everyday internet tasks, including internet banking, checking email and browsing online. It uses what is known as a 'trapdoor calculation', where the key is created by multiplying two very large prime numbers. To crack the key, you would need to factorise the resulting number, which is an intractable problem that would take many years to solve.

ISBN: 978-1-77669-240-8

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA