Task:

Explore how Public Key Cryptography works.

Using your Student ID, generate two primes (of the form 4x+1) encrypt it with your own private key and send this to a recipient with a Public Key and recover your original Student ID.

Use the Wiener attack to break your private key and is this way steal your identity by using your private key to encode another number and masquerade as you.

Making your own Keys:

Explore how Public Key Cryptography works and summarise this in your own words with particular attention to how the method generates these keys.

From your exploration above, generate Private and Public Keys using the number part of your student ID.

Using your student ID, determine how bits the number part can be represented with.

For a particular number of binary bits determine the number of prime numbers available in that bit range.

Using the nextprime function and your student ID create two prime numbers which are or the form 4n+1. Such that P1=4x1+1 and P2=4x2+1. Check that they have the same number of binary bits.

Use this to generate your private keys and encrypt your student ID.

Create a public key and use this to decrypt and recover your student ID.

Breaking the Keys:

Express both of these numbers as the sum of two squares (for example .

Draw these as two right angle triangles (a,b,c). Note that ,

Using the equations below: Let P1=C1 and P2=C2 and let the smallest value of the two squares be express the sides of each triangle as:

Test that both your triangle solutions meets the condition that: . Draw both triangles.

Multiply P1 and P2  together: P1 P2.  Can be expressed as the sum of two squares?

Using Euclids method of factorization show how the original prime numbers can be recovered using the sum of squares method.

For each of the Primes subtract 1 and multiply these together:

Show that if are known, that the original primes P1 and P2 can be recovered.

Using your public key, show how your private keys can be recovered using the Wiener attack by recovering P1 and P2 .

As the villain armed with this information, pretend to be you and send a different encrypted Student ID (not yours) encrypted with the recovered key. And use the same public key as earlier to recover the false Student ID.