**RSA Assignment: Self-Marking Sheet**

**Please Complete (by grading yourself under the first 3 headings and providing justification for the mark you awarded yourself) and upload.**

**Student name: Patrick McDonnell D00006968**

**Implementation (8 marks)** (Have you fully implemented the chosen Cryptosystem? Your application should be capable of (i) Key generation; (ii) encryption & (iii) decryption? **What size of message can it encoded/ decode? Any limitations? Is it well written/efficient & commented?** )

It has fully implemented the BigInteger system for Rsa cryptography.  
it generates keys both public and private.

Its can encrypt the string message taken in from a user

And can then decrypt the message using the keys generated above to display the original message taken in from the user.

It can encode/decode message of any size, I do this by breaking up the message into smaller chunks and storing them in an arrayList then iterating through it to encode/decode an display the message.

It is an efficient as I can make it utilizing methods to reduce the redundant code.

It is well commented with java doc in place for each of understanding.

**Award myself 8 marks**

**Innovations (4 marks)** (Does your implementation contain any self-authored methods / additional securities or other features that warrant additional marks? Explain.

Well my code does break up the data, so that method was self generated. But as to other functionality it was done by utilizing the methods inherent in the BigInteger class.

Also has a method for encrypting/decrypting. But again utilizing the BigInteger methods.

My code also uses java.security.SecureRandom; this is to provide a more cryptographically sound random number than is less likely to be guessed.

**Award 3 marks**

**Documentation (4 marks) (**How well does your documentation meet the requirements of providingdetails of (i) the methodology/ structures used in your implementation; (ii) **any limitations in your program, due to assumptions made;** (iii) any problems encountered and (iv) output from examples used to test your program. **)**

Documentation goes in depth into how I utilized the methodology and what code was used to enact each part of it. With examples provided as well as a thorough explanation of it.

Limitations were detailed within my documentation. Yet some of which I have since overcome. But left in to show that they were inherent.

Problems encountered are also covered in detail outlining any issues I had whilst completing the program.

Output from the code is provided and screenshots provided showing the code in action. There is also what was input into the code so you ca verify that it works.

**Award 4 marks.**

**Demo (4 marks) (**You will also be required to present your application. This will involve (i) explaining your code; (ii) providing details of the methodology used; (iii) discussing any limitations in your program, due to the assumptions made; (iv) highlighting any problems encountered; (v) a walk through output from examples used to test your program and (vi) answer questions.) **You will provide this mark after your demo.**

**---------------------------------------------------------------------------------------------**

**This assignment is entirely my own work and any code incorporated was written by me. I have advise my lecturer where this is not the case.**

**Signature:**