

14th February 2026

9:02 p.m.

I rewrote the code for generating prime numbers and got rid of the Miller Rabin test as well as Euler totient function from my code. Euler's totient factoring speed, when the bits are set at 1000 and above (2000 bits being what is used in the real-world RSA encryptions) is too long and there is a keyboard interrupt for that reason. There is also a difference in the user interaction which now requires the user to input the public key component "e" to encrypt the message they put into the programme when first prompted after the prime numbers are generated; and also requires the user to input the value of "d" which is part of the private key used to decrypt the message.

The programme has been completed, and the few times I tested it out, it has worked out perfectly well. I learned about totient factoring speed and that the more bits are used, the longer and or nearly impossible it is for it to compute and thus the system stops working (Keyboard Interrupt).

Nothing really remains unclear or challenging so far. I do tend to forget the power, base and modulus operations from time to time but a little reading and watching videos on YouTube always refreshes my memory.

I will attempt to build a user interface which isn't text based like it is now where you can get the output in the terminal. Assuming it all works out, it should be finalised by next weekend.

I spent about ten hours working on the project this week.