Lab3

Joseph Potapenko

October 2025

1 Part 1 Screenshot

Reference Figure 1 below

2 Part 2 Answer

I did what the slides said to do step by step, just in python. But on a real note, I took n (the modulus) from the public key, and then I factored it into p and q, the two prime factors, and then used it to find the lamda of n by finding the lowest common multiple of p-1 and q-1. Then, I solved for d using the provided modinv function with e and lamda n, which gives us d as the modular multiplicative inverse of e modulo lamda n. And then we solve for the plaintext integer using the dcipher function M = C to the power of d mod n, and turning that from the byte integer to text gives us the message: b'YouDonePassed!!'

3 Part 3 Answer and Figures

Reference Figures 2 and 3 below. Figure 2 is the data, and Figure 3 is the graph.

Since the amount every 10 steps increases exponentially, I cannot give a concrete answer, but I can hazard a guess. Since 104 was an average of approximately half an hour, 114 could be a few hours, 124 could be around half a day, and 134 could be around more than a day. I would estimate 144 is possible, but anything above 150-160 would be unreasonable in my opinion, but it is hard to have an accurate estimate without having a crap ton of time to actually test the program.

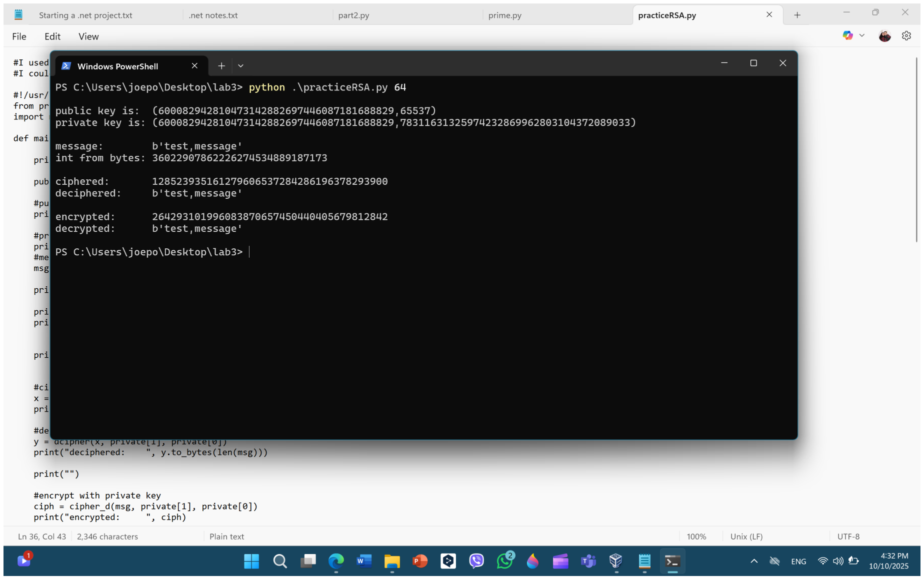

Figure 1: Enter Caption

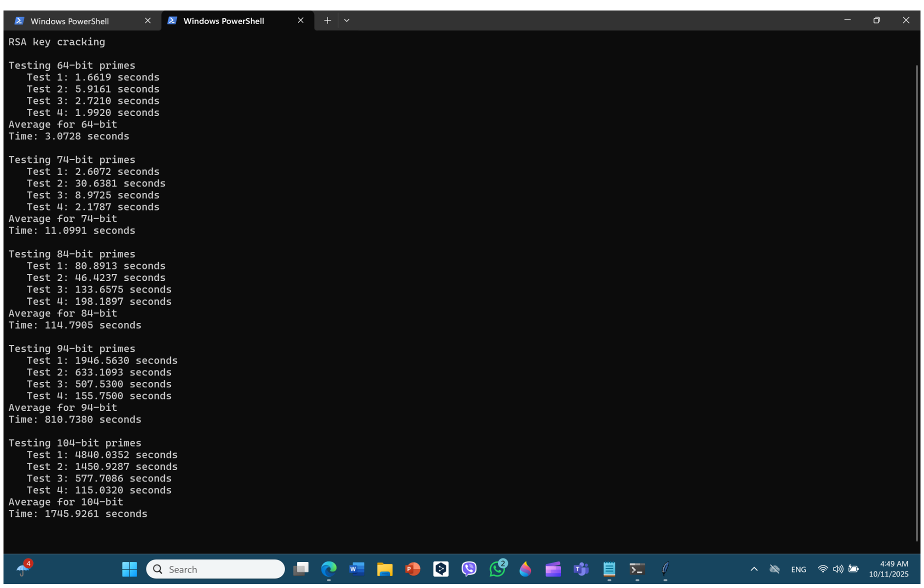

Figure 2: Enter Caption

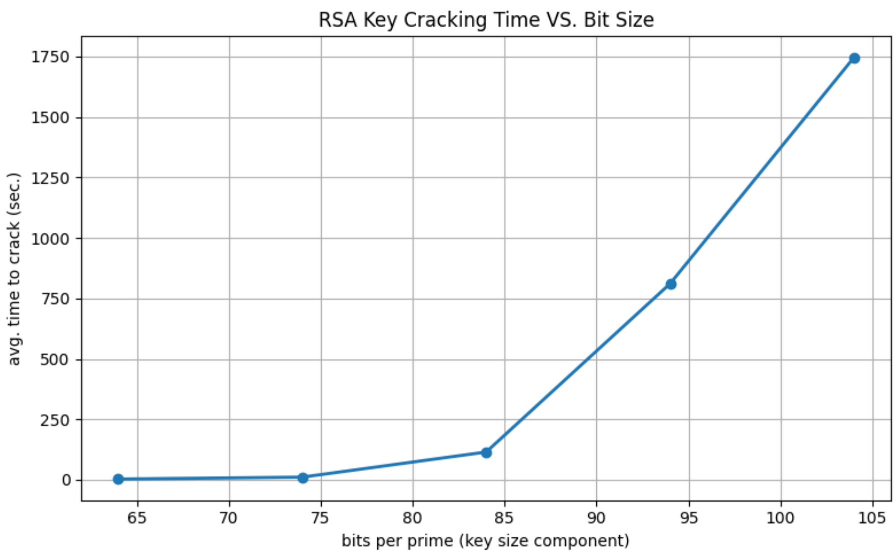

Figure 3: Enter Caption