

Lab3

Joseph Potapenko

October 2025

1 Part 1 Screenshot

Reference Figure 1 below

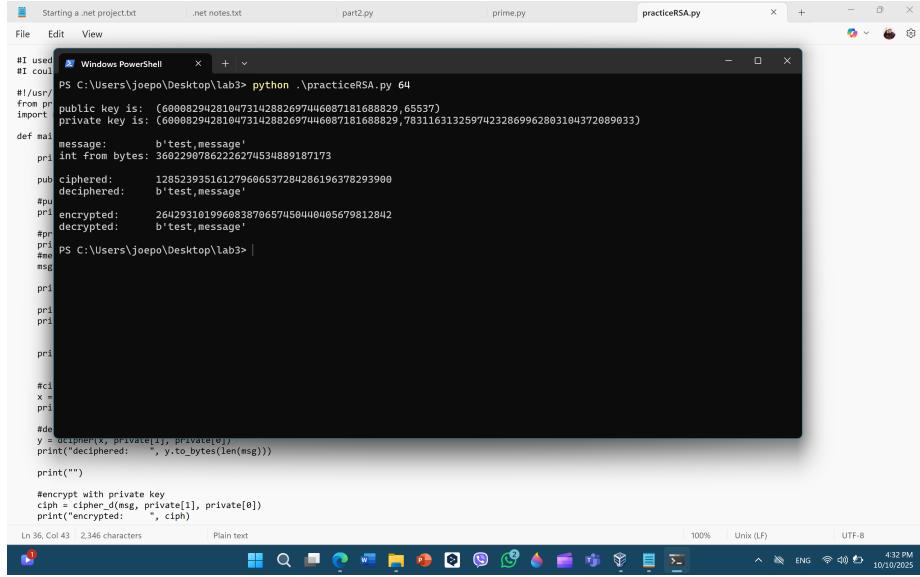
2 Part 2 Answer

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 lambda 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 lambda n , which gives us d as the modular multiplicative inverse of e modulo lambda 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.

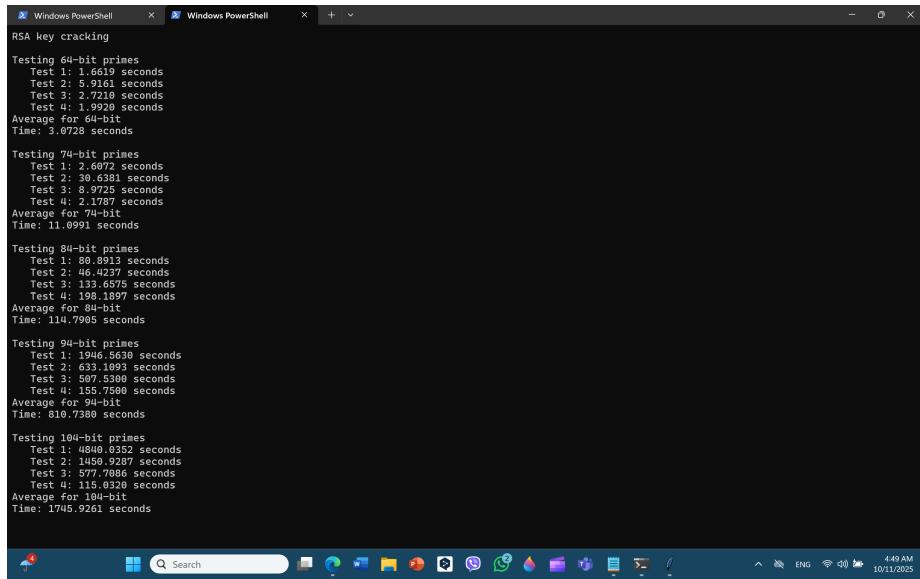


```

#I used    Windows PowerShell
#I could
PS C:\Users\joepo\Desktop\lab3> python .\practiceRSA.py 64
#I used    Windows PowerShell
#I could
from pr
import
public key is: (600002942810473142882697446887181688829, 65537)
private Key is: (600002942810473142882697446887181688829, 78311631325974232869962803104372089033)
def mai
    message:      b'test,message'
    pri
    int from bytes: 36022907862226274534889187173
    pub
    ciphered:    130523935161279606537284286196378293900
    #pu
    deciphered:  b'test,message'
    #pr
    encrypted:   261293101996083870657450440405679812842
    #pr
    pri
    PS C:\Users\joepo\Desktop\lab3> |
#ne
#m
msg
pri
pri
pri
pri
#cl
x =
pri
#de
y = decipher(cipher, private[1], private[0])
print("deciphered: ", y.to_bytes(len(msg)))
print("")
#encrypt with private key
ciph = cipher_d(msg, private[1], private[0])
print("encrypted: ", ciph)
Ln 36, Col 43  2,346 characters

```

Figure 1: Enter Caption



```

RSA key cracking
Testing 64-bit primes
    Test 1: 1.6619 seconds
    Test 2: 5.9161 seconds
    Test 3: 2.7210 seconds
    Test 4: 1.9920 seconds
    Average for 64-bit
    Time: 3.0728 seconds

Testing 74-bit primes
    Test 1: 2.6672 seconds
    Test 2: 30.6381 seconds
    Test 3: 8.9725 seconds
    Test 4: 1.1987 seconds
    Average for 74-bit
    Time: 11.0991 seconds

Testing 84-bit primes
    Test 1: 80.8913 seconds
    Test 2: 133.6597 seconds
    Test 3: 133.6595 seconds
    Test 4: 198.1897 seconds
    Average for 84-bit
    Time: 114.7905 seconds

Testing 94-bit primes
    Test 1: 1946.6339 seconds
    Test 2: 633.1093 seconds
    Test 3: 507.5300 seconds
    Test 4: 155.7500 seconds
    Average for 94-bit
    Time: 810.7380 seconds

Testing 104-bit primes
    Test 1: 4840.0352 seconds
    Test 2: 1456.9287 seconds
    Test 3: 577.7086 seconds
    Test 4: 115.0320 seconds
    Average for 104-bit
    Time: 1745.9263 seconds

```

Figure 2: Enter Caption

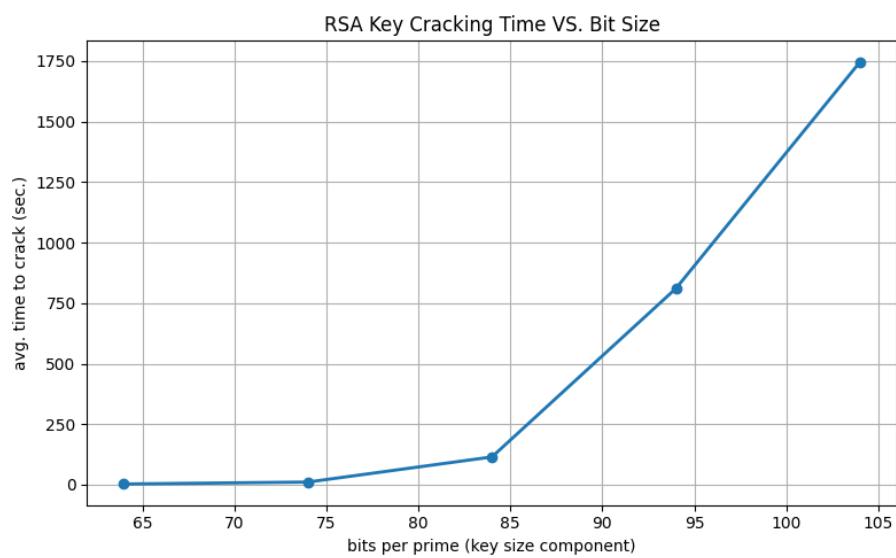


Figure 3: Enter Caption