**INDEX**

INTRODUCTION

HOW THE CODE WORKS?

BACKGROUND

RSA Algorithm

How This Works in Practice?

RSA ALGORITHM

Generating Keys

Encrypting

Decrypting

CODE

BIBLIOGRAPHY

INTRODUCTION

AIM

The project aims to create a working code for the RSA-algorithm used in Cryptography.

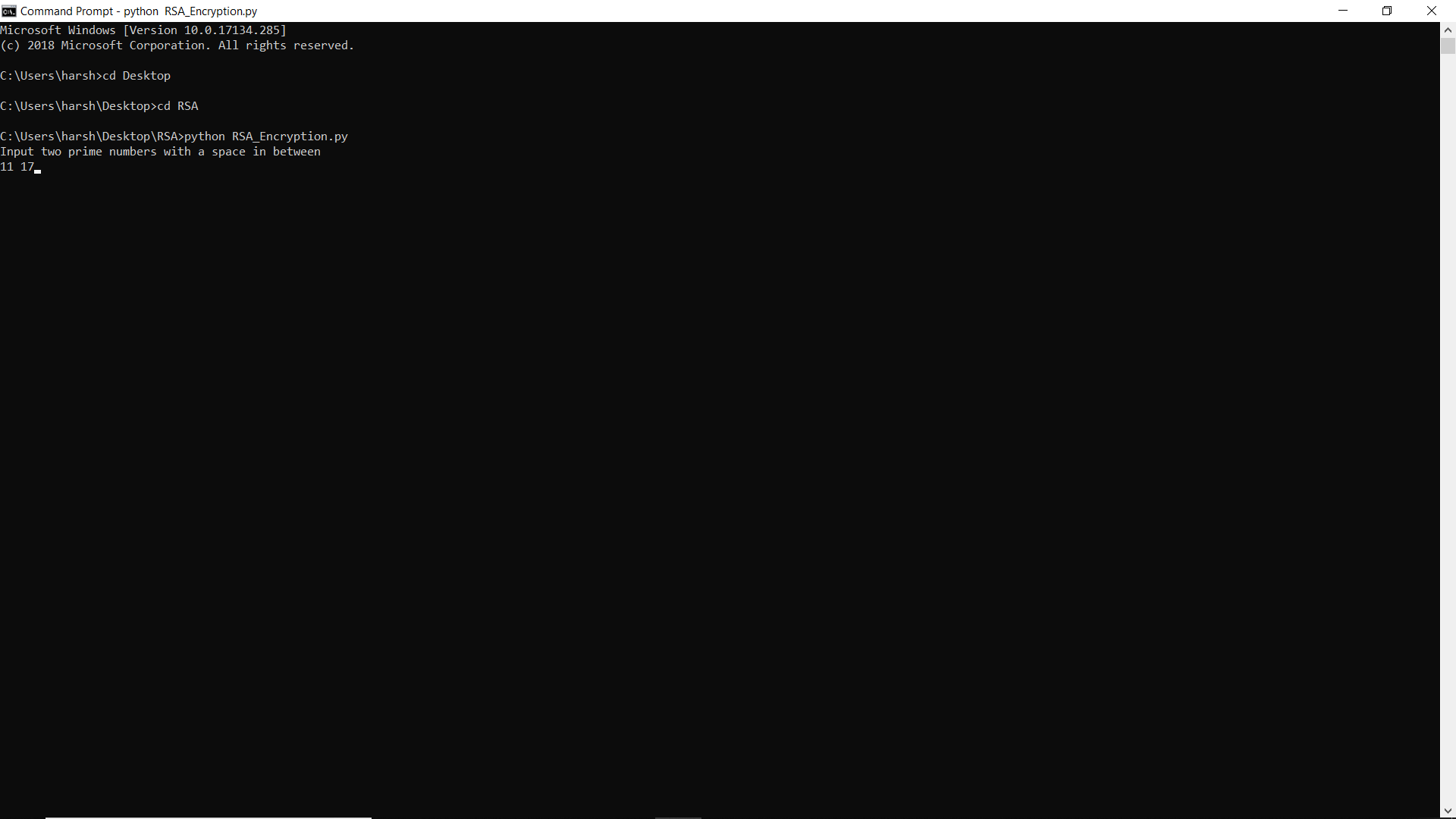
MOTIVATION

The following were the motivation to choose RSA-Algorithm as our project :\_

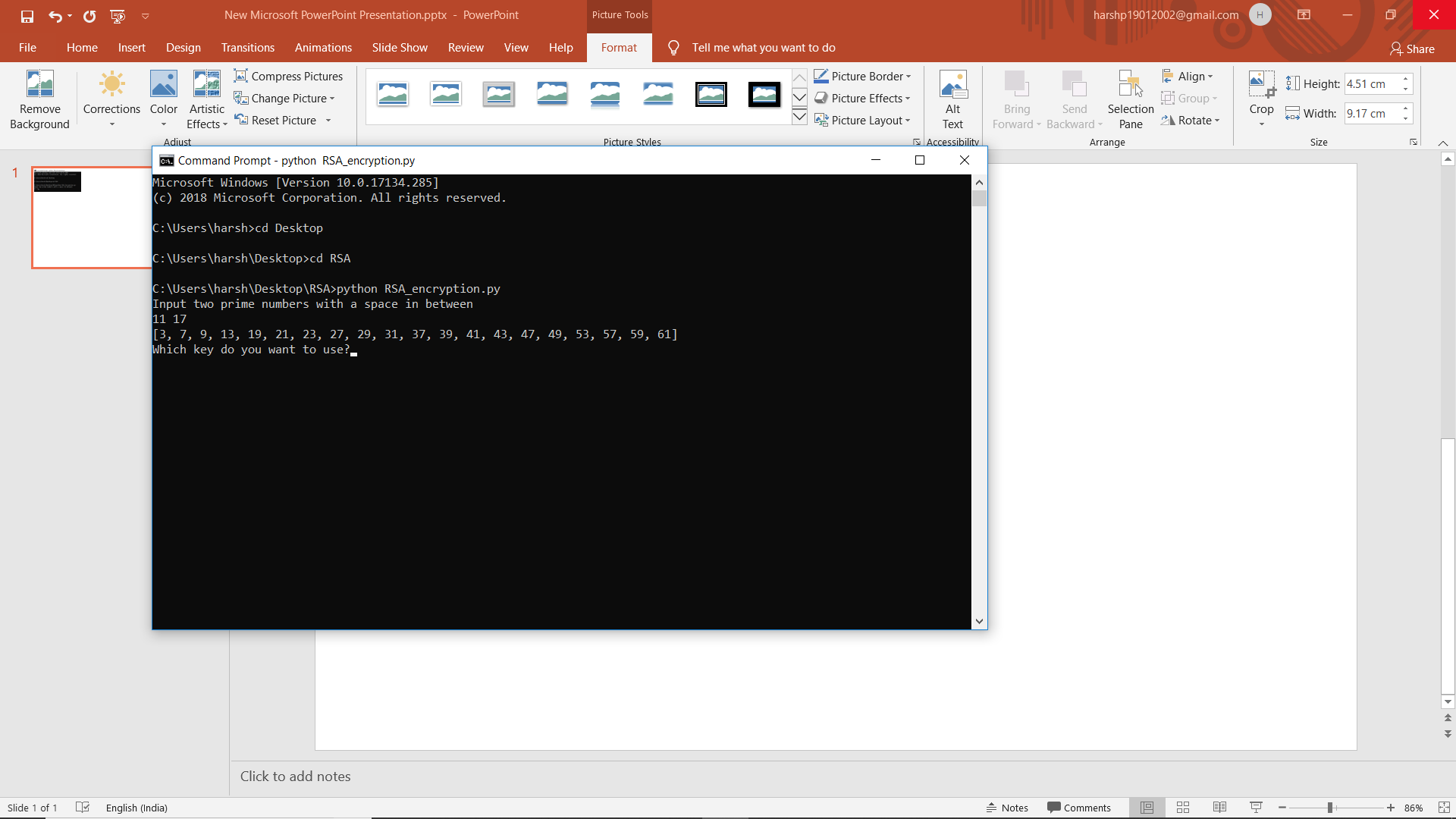
* We were introduced to cryptography in class with basic cipher techniques like caesar cipher and vignere cipher.
* Concept of Public key and Private key was discussed with us so we had a very basic idea of how this worked.
* We had to find GCD in between the algorithm so we also used Euclid’s Algorithm :D .

HOW THE CODE WORKS?

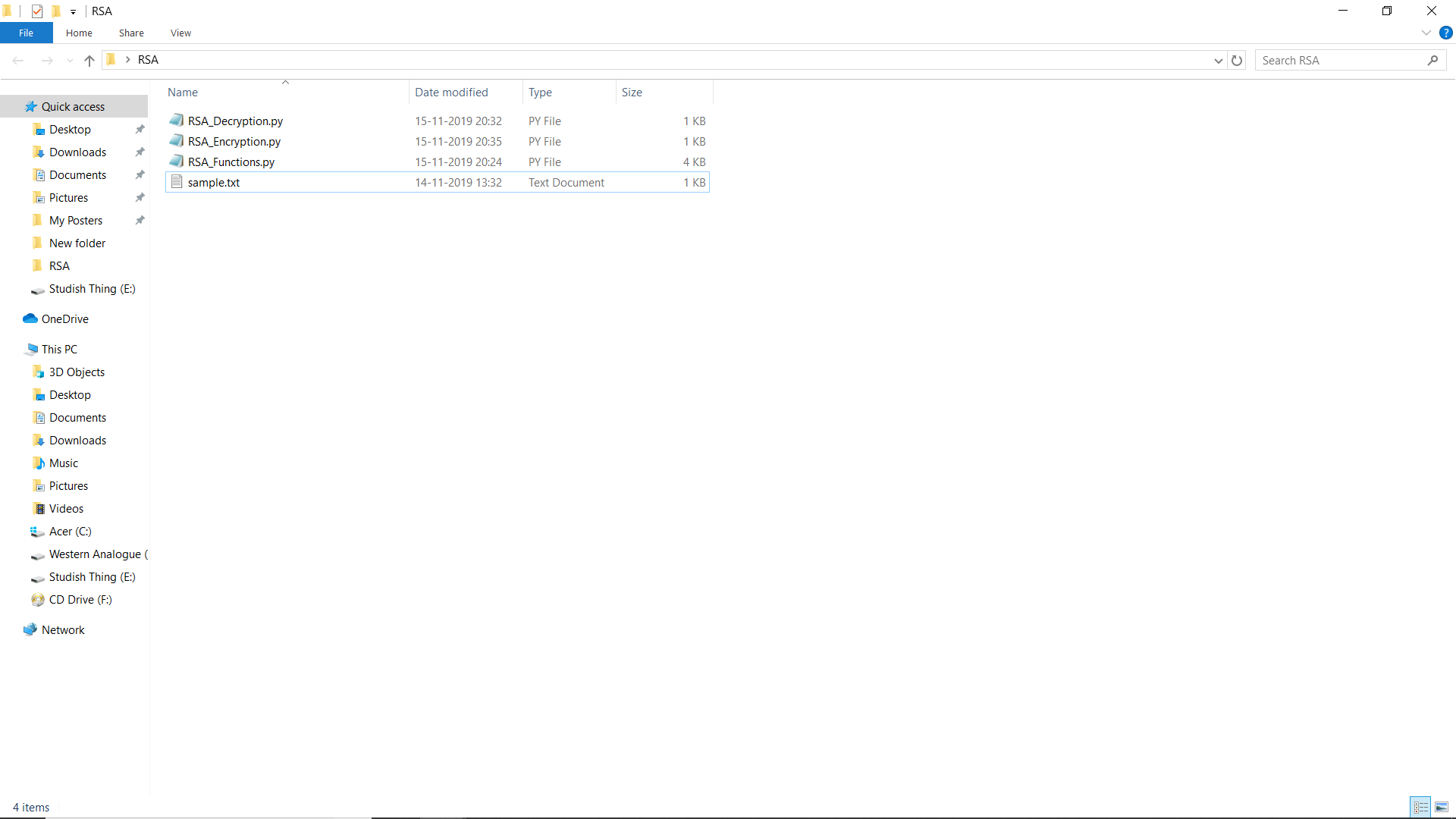
1. Run ‘RSA\_Encryption.py’
2. Takes two prime numbers as input.



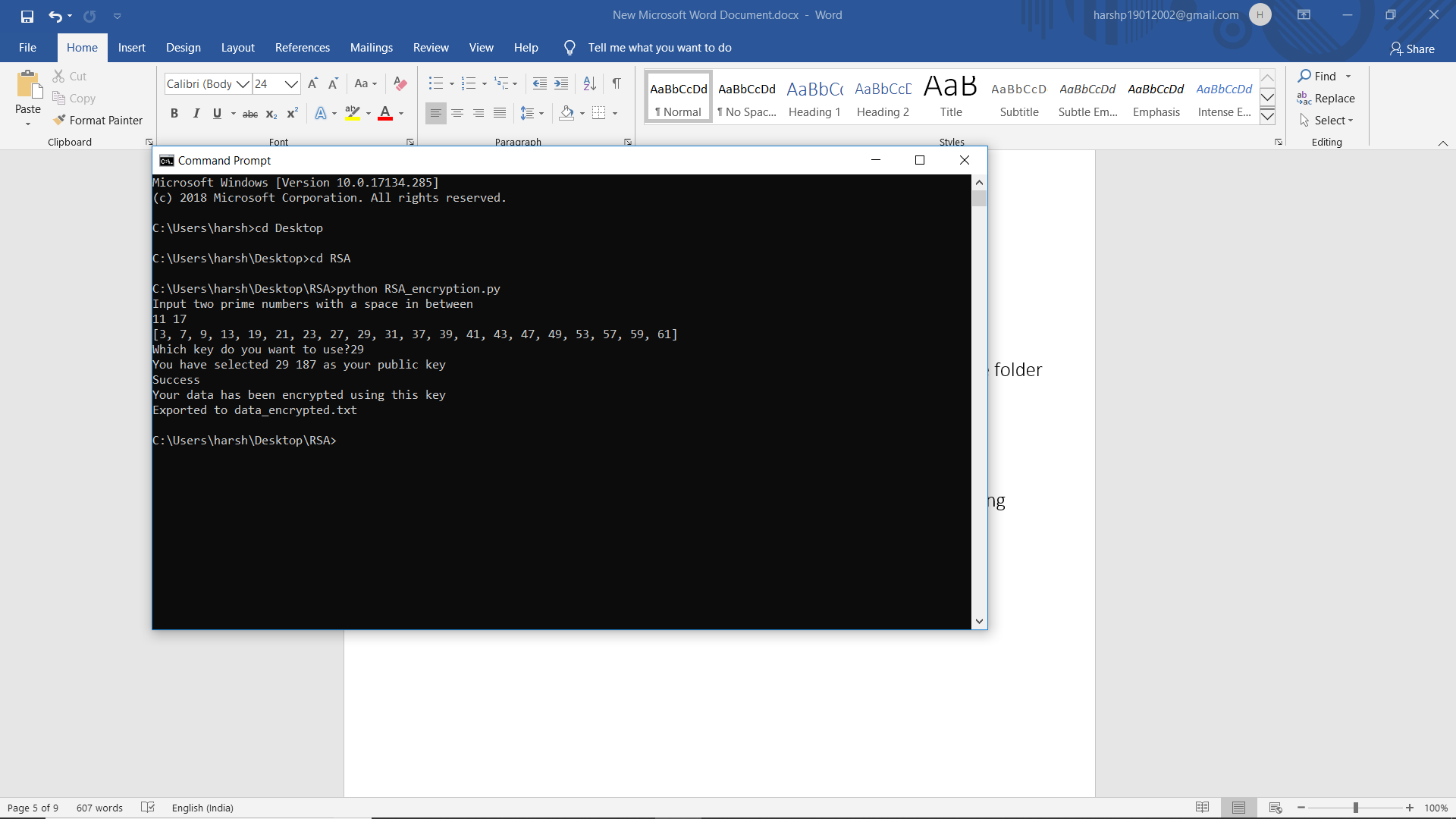
1. Generates various compatible public keys for these prime numbers



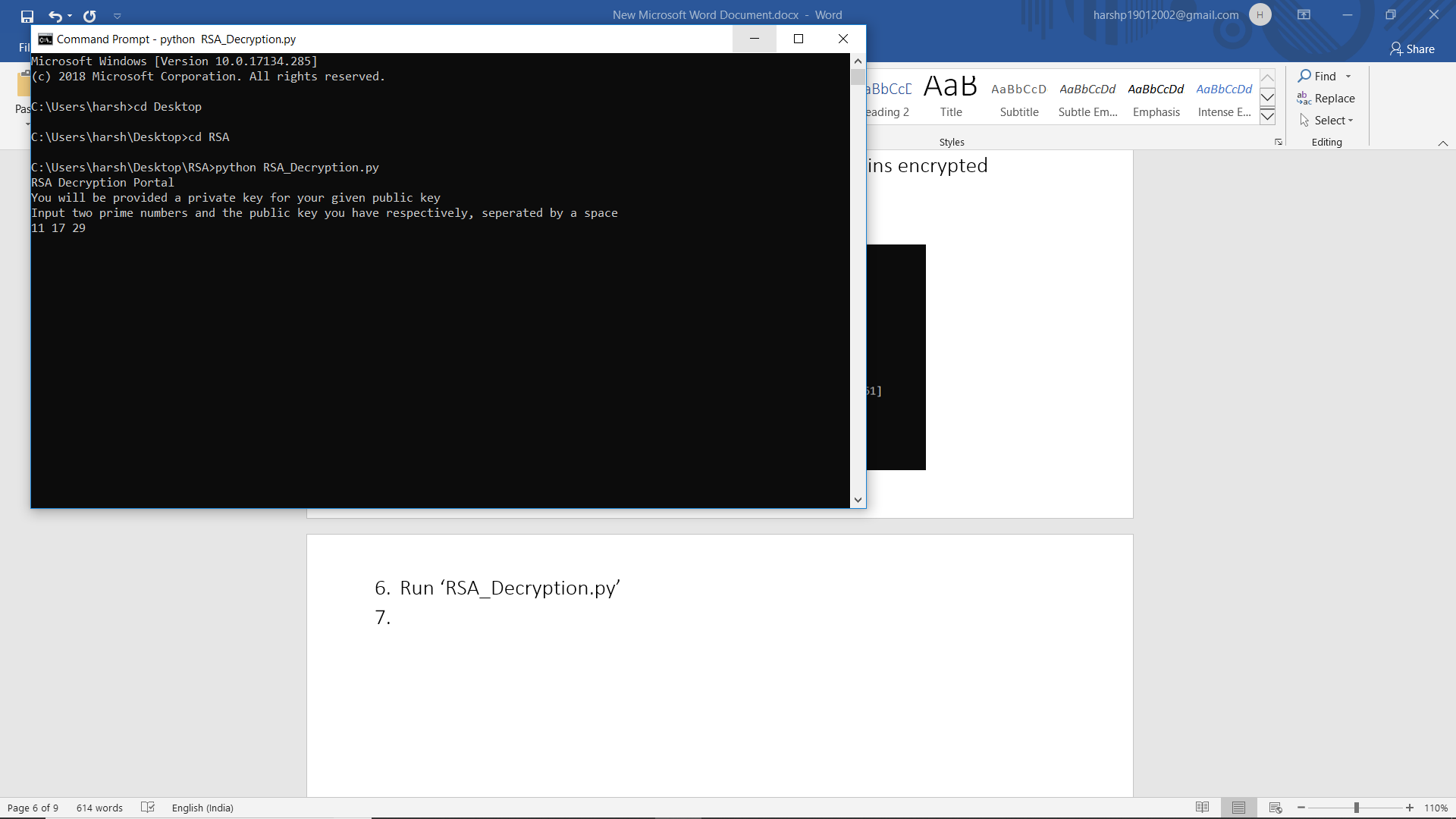
1. Data which has to be encrypted to be put in “sample.txt” in the same folder



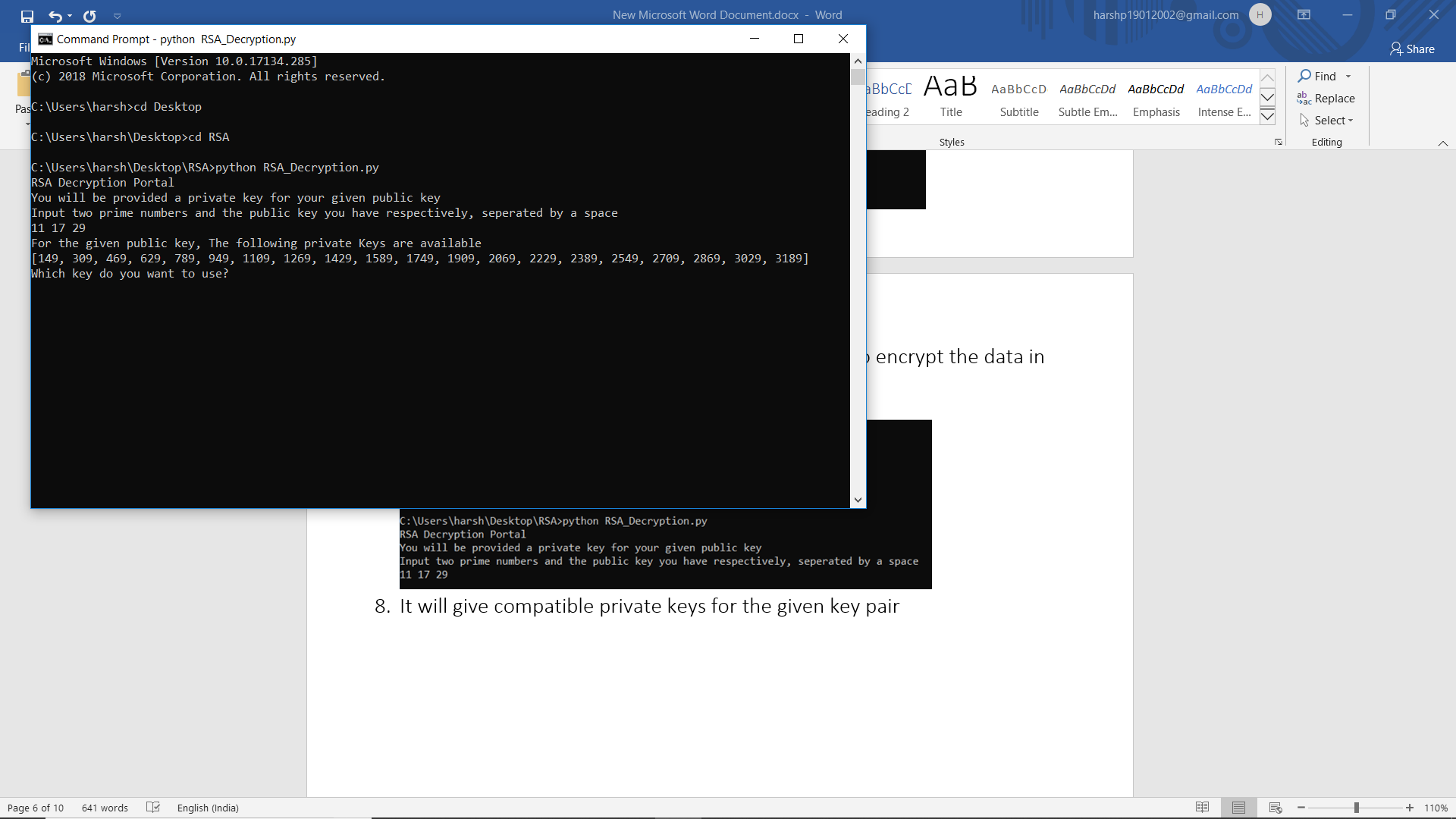
1. The proamme encrypts the data and exports two files one containing plaintext (“Data\_Wordsonly.txt) and the other contains encrypted data(“Data\_Encrypted.txt)



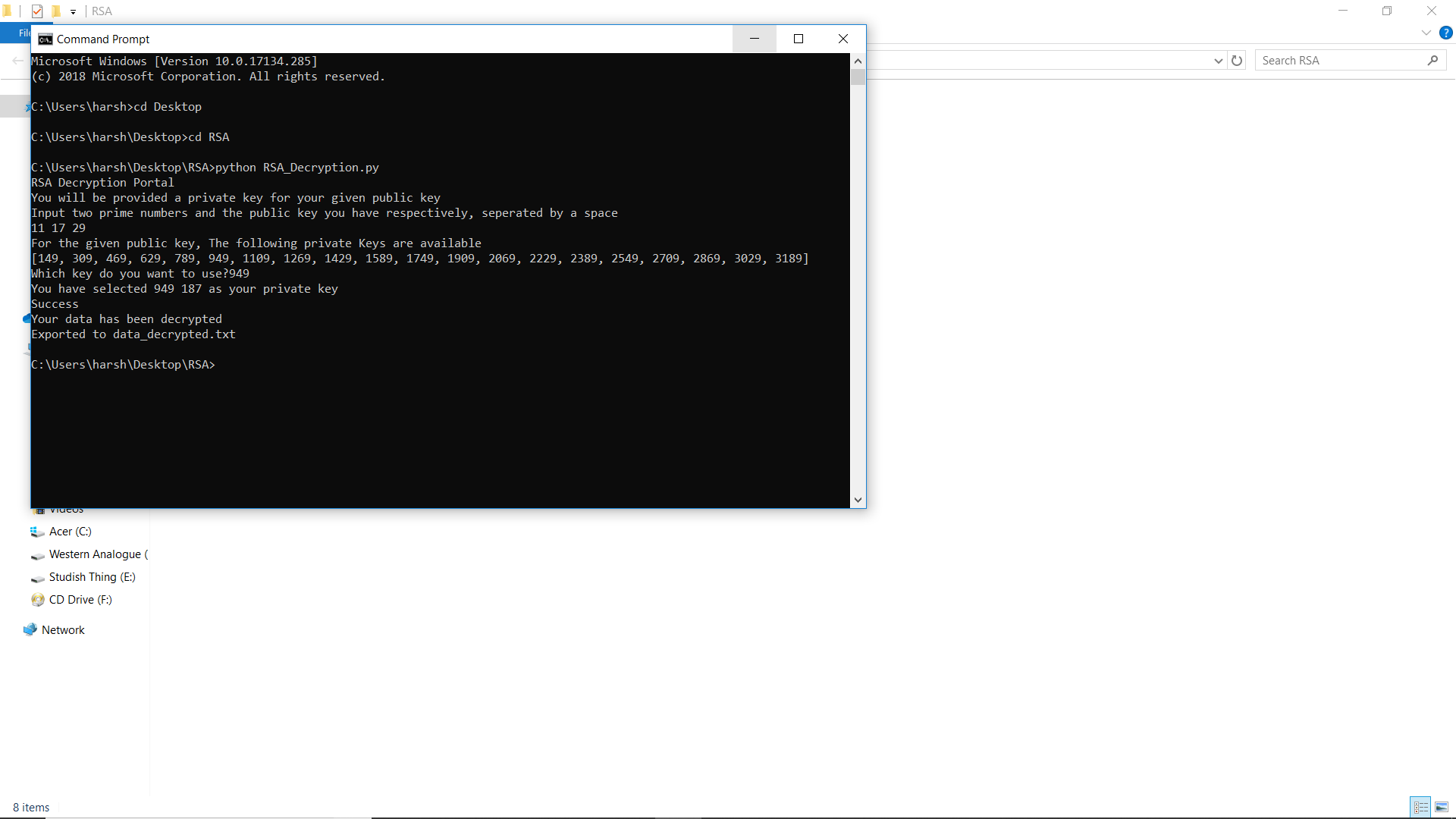
1. Run ‘RSA\_Decryption.py’
2. Input Prime numbers and public key which is used to encrypt the data in “Data\_Encrypted.txt”



1. It will give compatible private keys for the given key pair



1. It will decrypt the data with the suitable key pair and export it in “Data\_Decrypted.txt”

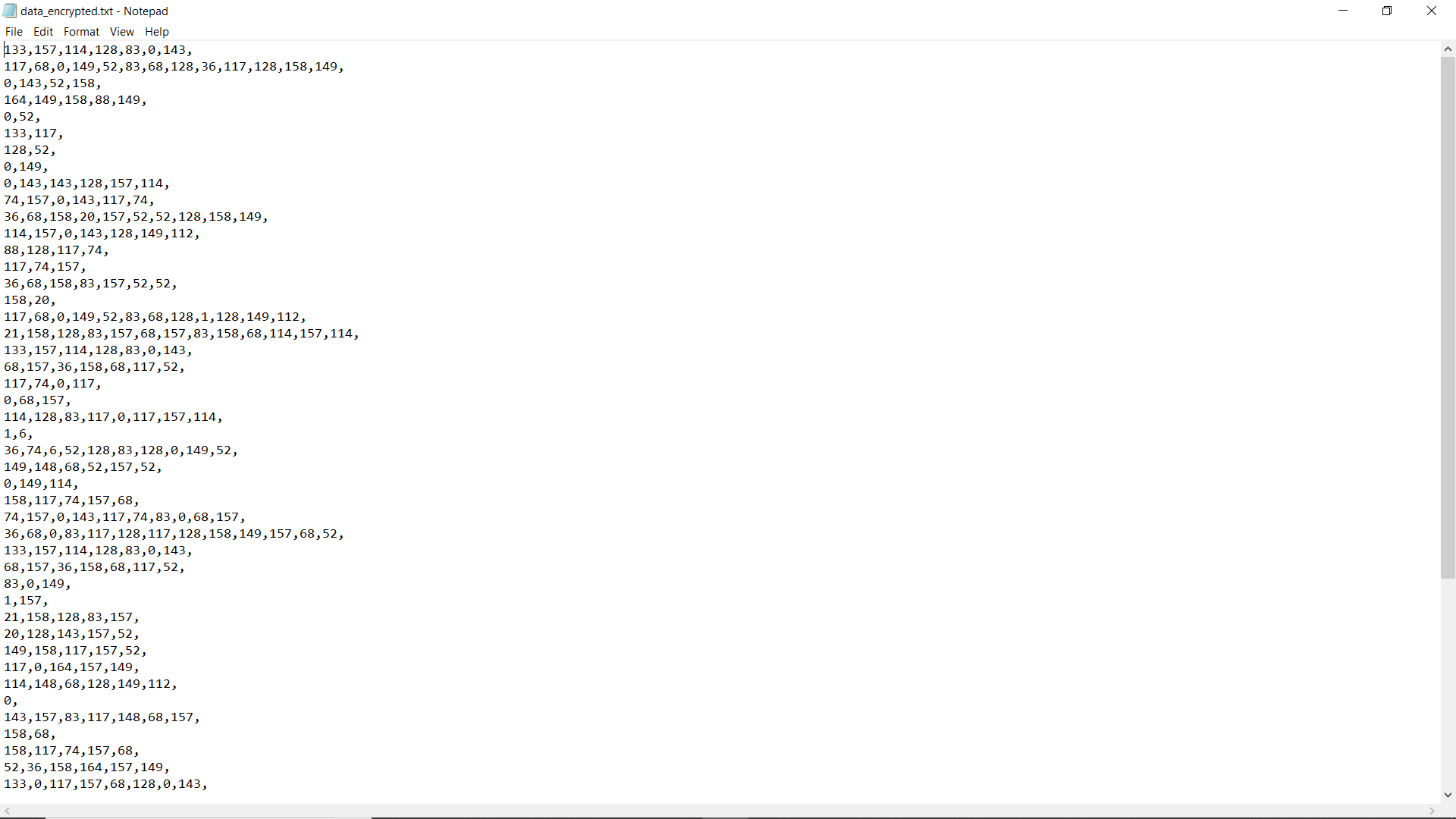
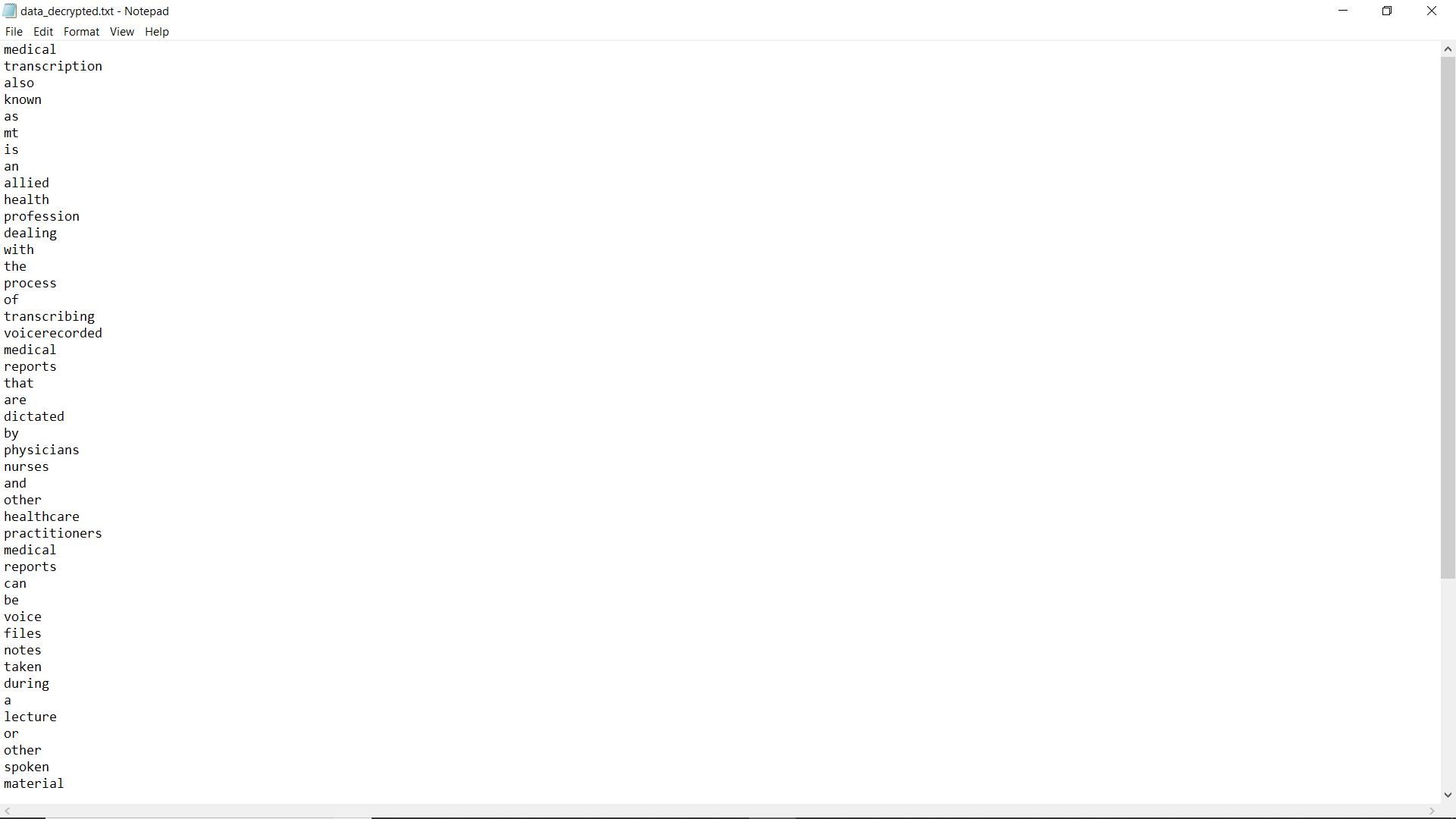


**NOTE:-**

**In Actual RSA Algorithm the prime numbers that we take are very huge so that factorization is difficult.**

**Our programme is not as efficent as the actual one so it is working very slow for prime numbers greater than 5 digits.**

**So input to be taken in as 3-4 digit prime numbers.**

* Encrypted data and decrypted data will look like this
* 

ENCRYPTED DATA

DECRYPTED DATA

BACKGROUND

RSA Algorithm

**RSA (Rivest–Shamir–Adelman)** is an algorithm used by modern computers to encrypt and decrypt messages.

It is an asymmetric cryptographic algorithm.

Asymmetric means that there are two different keys.

This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private.

The algorithm is based on the fact that finding the factors of a large composite number is difficult.

HOW THIS WORKS IN PRACTICE?

For example two individuals want to communicate secretively.

* First, they each need to set up their own key pairs and share the public key with one another.
* The two entities need to keep their private keys secret in order for their communications to remain secure.
* Once the sender has the public key of their recipient, they can use it to encrypt the data that they want to keep secure.
* Once it has been encrypted with a public key, it can only be decrypted by the private key from the same key pair.
* **Even the same public key can’t be used to decrypt the data.**

RSA-ALGORITHM

1. GENERATING THE KEYS

* We need two prime numbers, say p and q.
* We need to find the number of numbers less than N which satisfy

gcd(x,N)=1

* Name this X
* X can be easily calculated as

* Now we can find E(encryption key)
* All numbers which satisfy the following properties can be used as E
* NOW, we need to pair this key up, by finding a suitable D
* D would be acceptable if it satisfies the following condition
* Now we have public key as (E,N) and private key as (D,N)

1. Encrypting the Data

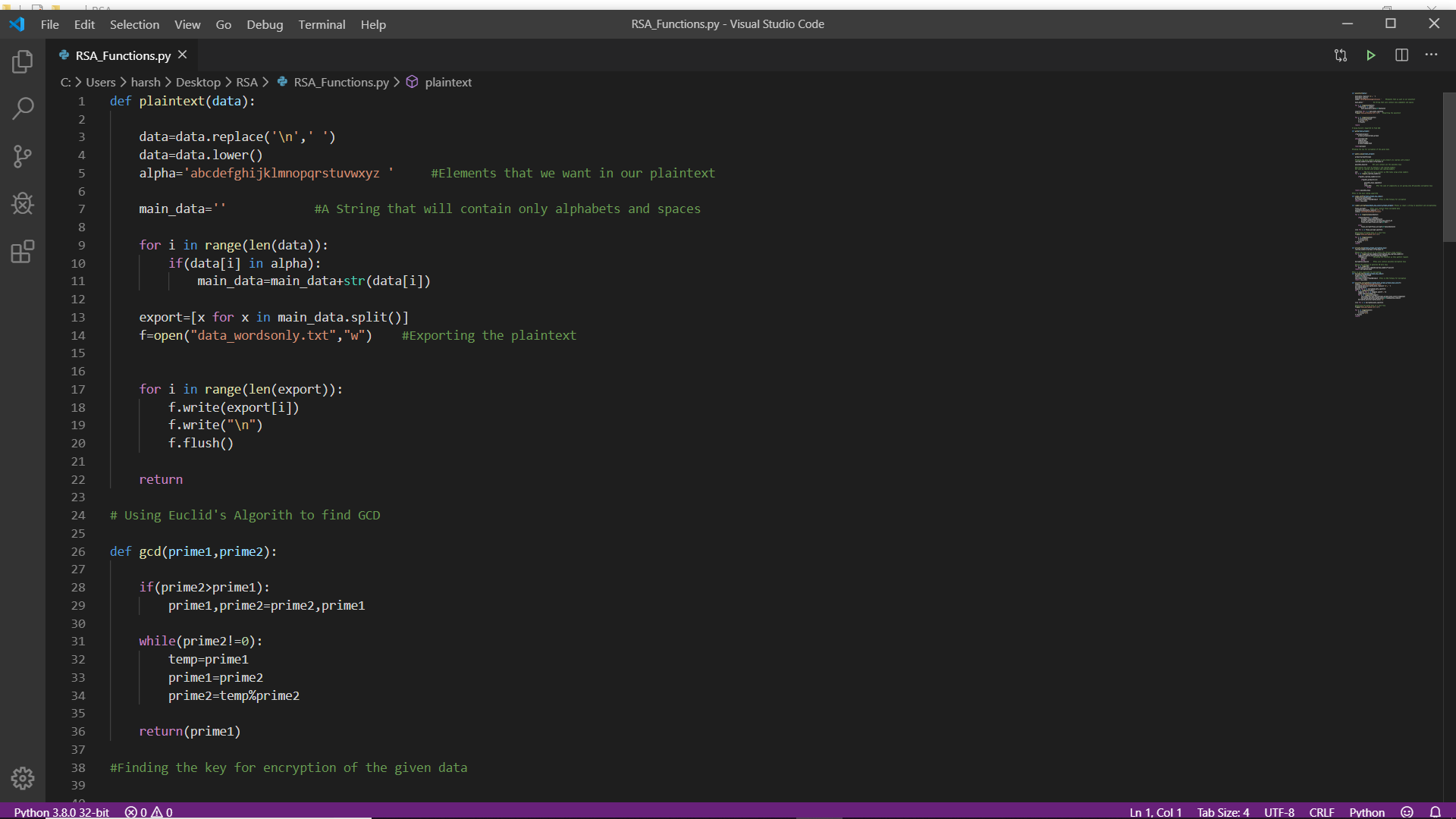
* Data can be encrypted using the followinf formula.
* For example we have to decrypt a number say M
* Encrypted Number would be

1. Decrypting the Data

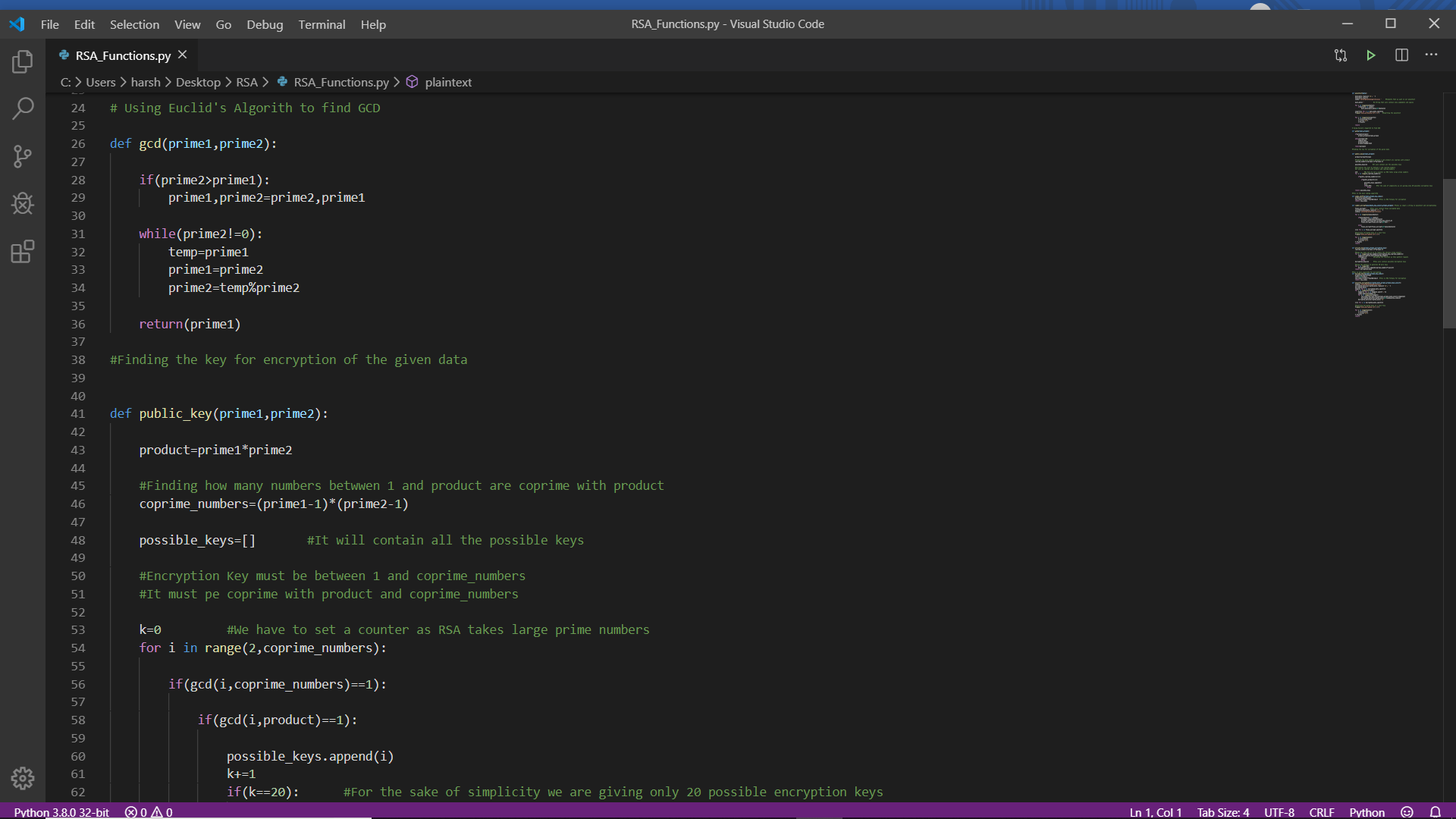
* Data will be decrypted with the same formula

CODE

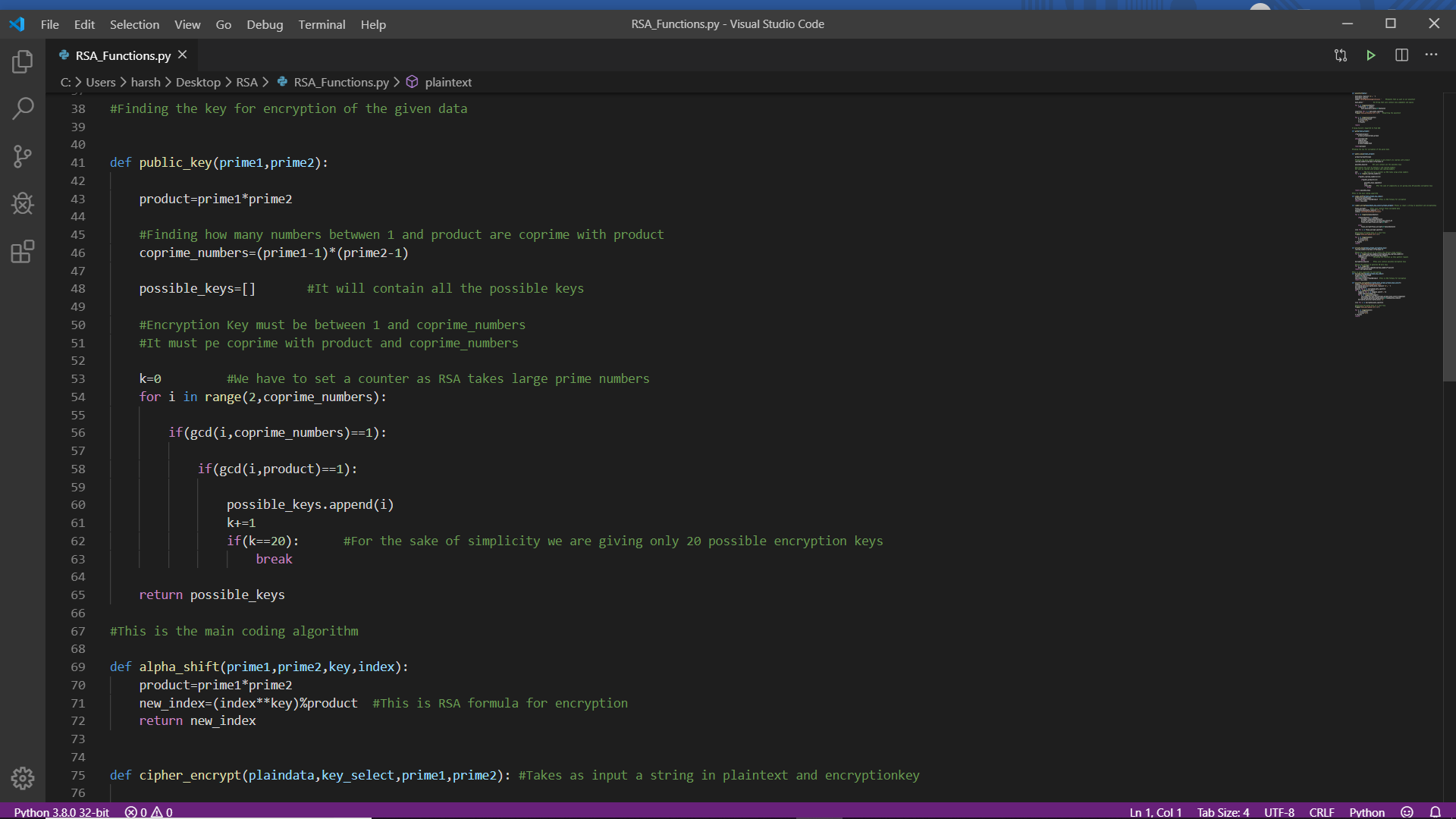
1. PlainText

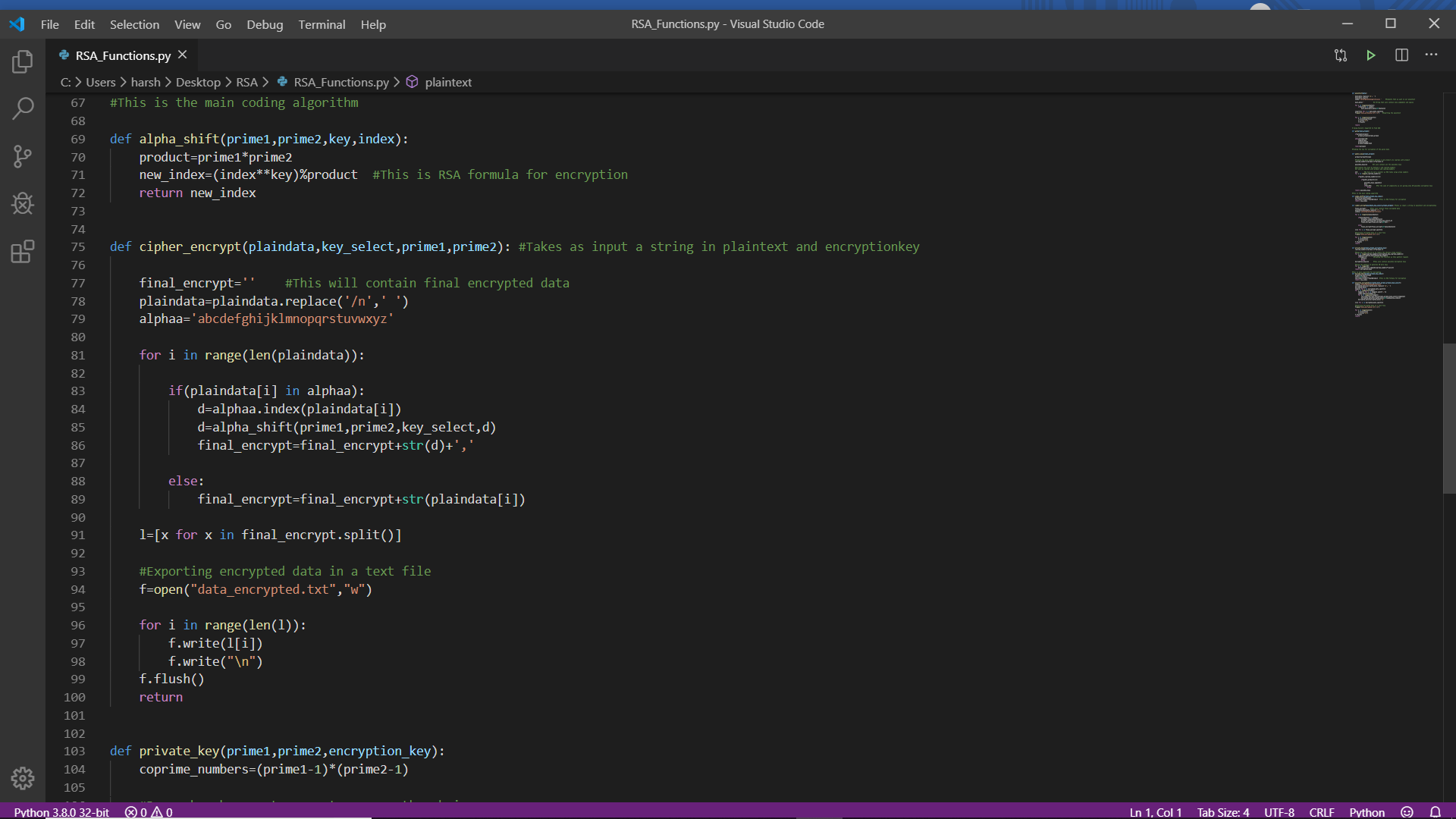


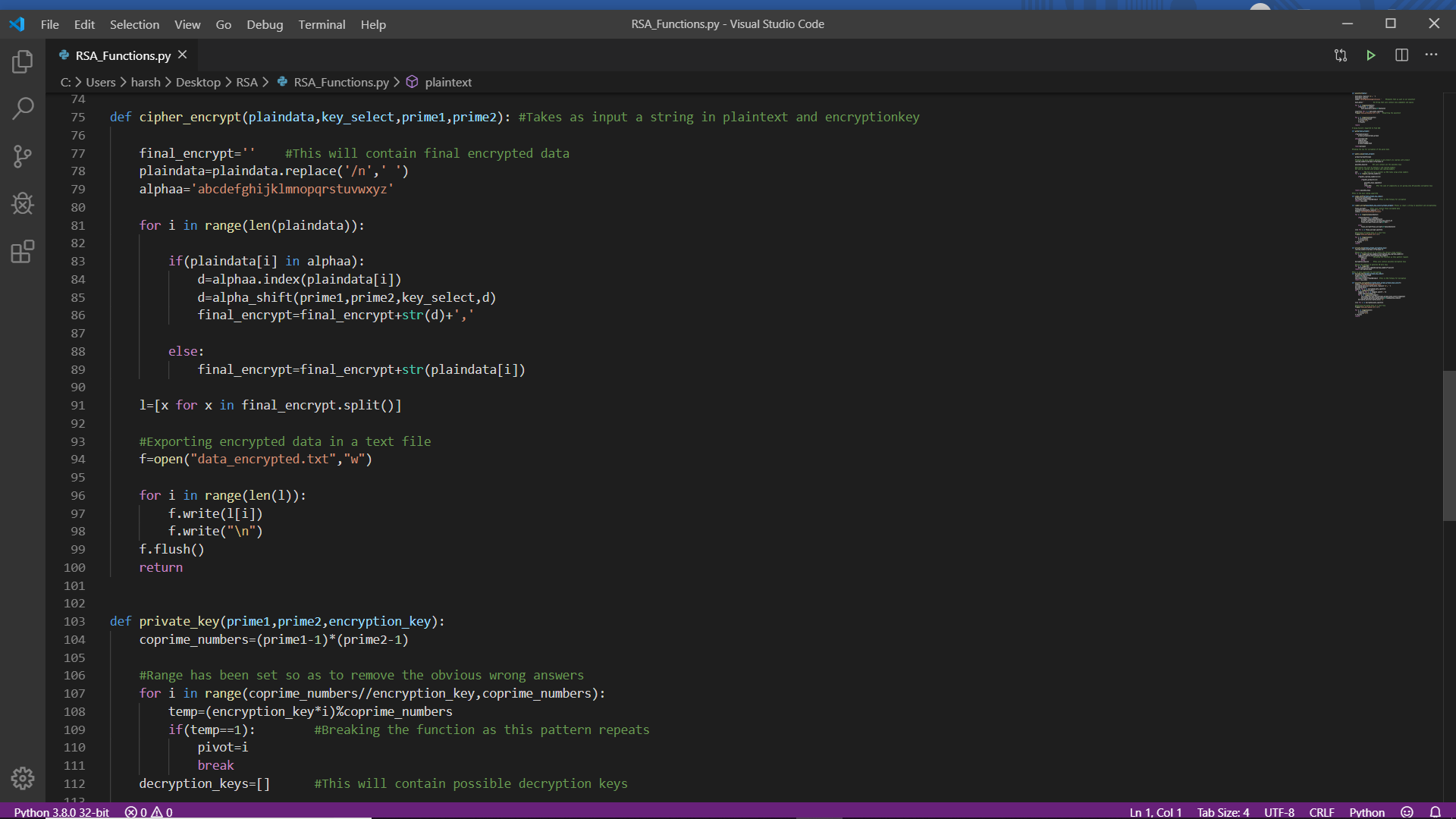
1. GCD (Euclid’s Algorithm)



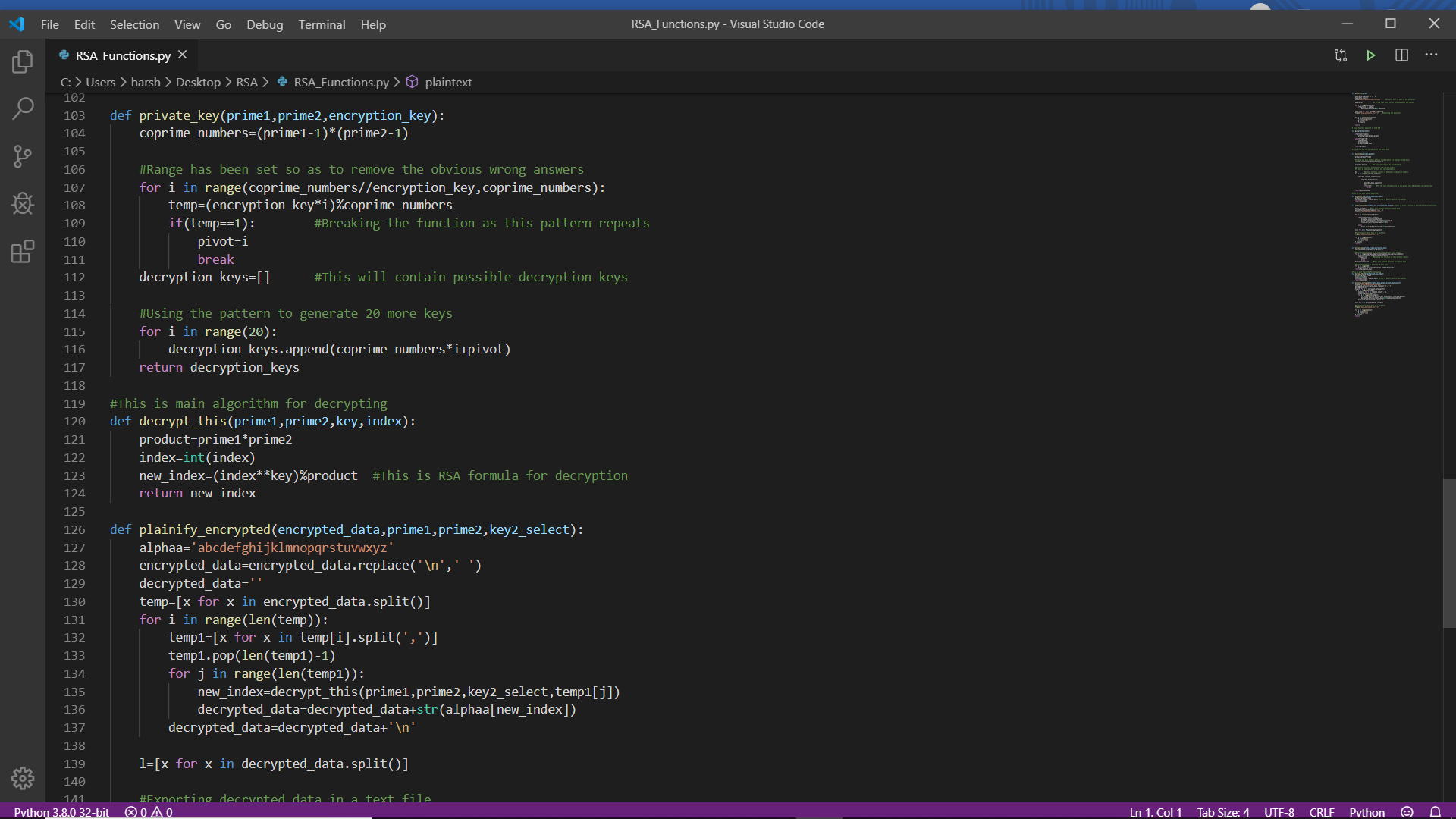
1. Public Key (Finding the Public Key)



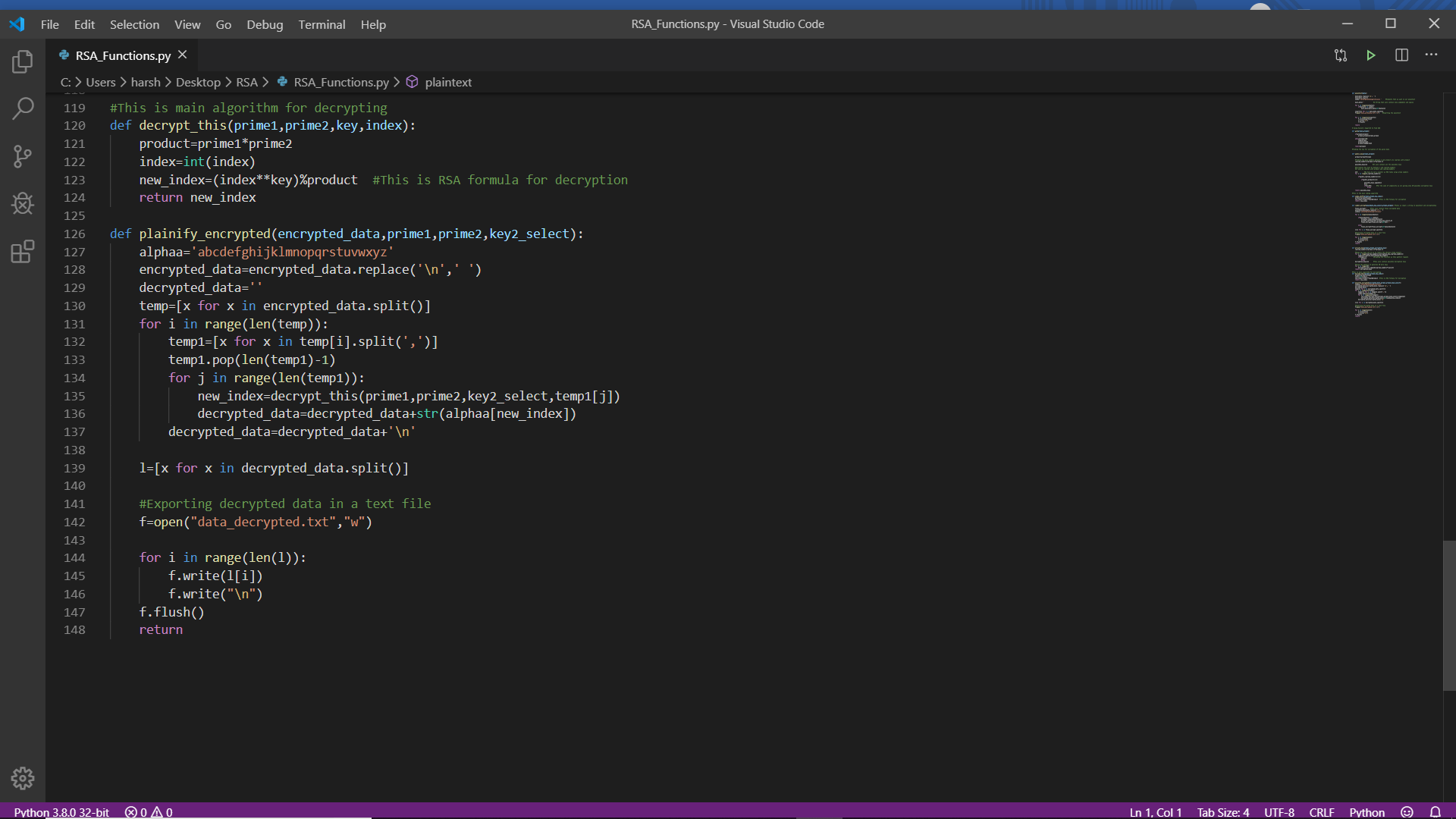
1. Main Encryption
2. Cipher\_Encrypt (Encrypts Whole Data)



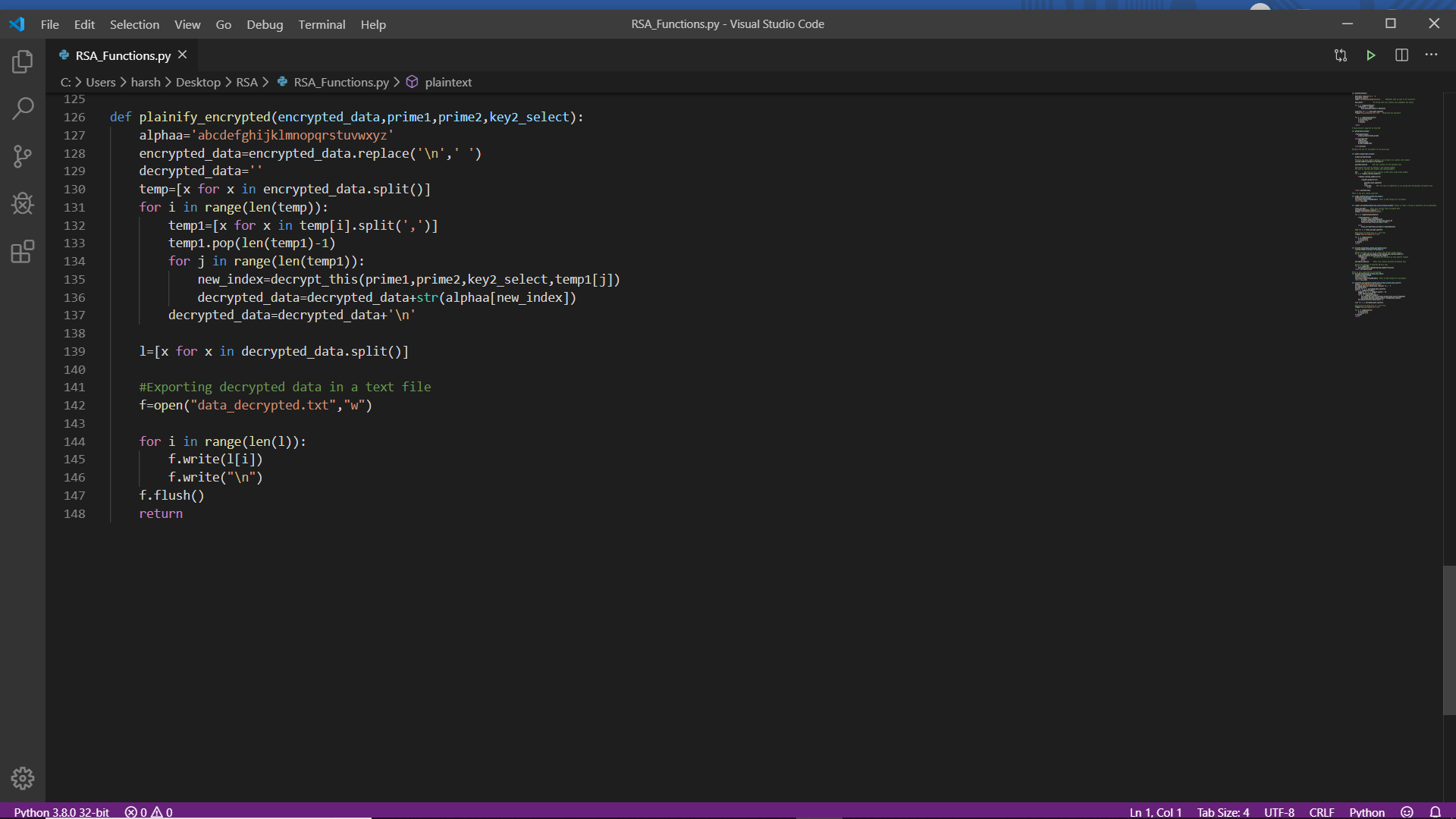
1. Private\_Key (Finds Private Key)



1. Decrypt\_This (This is the main decrypting algorithm)



1. Plainify\_Encrypted (This decrypts the encrypted data)



BIBLIOGRAPHY

* <https://www.comparitech.com/blog/information-security/rsa-encryption/>
* <https://simple.wikipedia.org/wiki/RSA_algorithm>