Steven Fuller

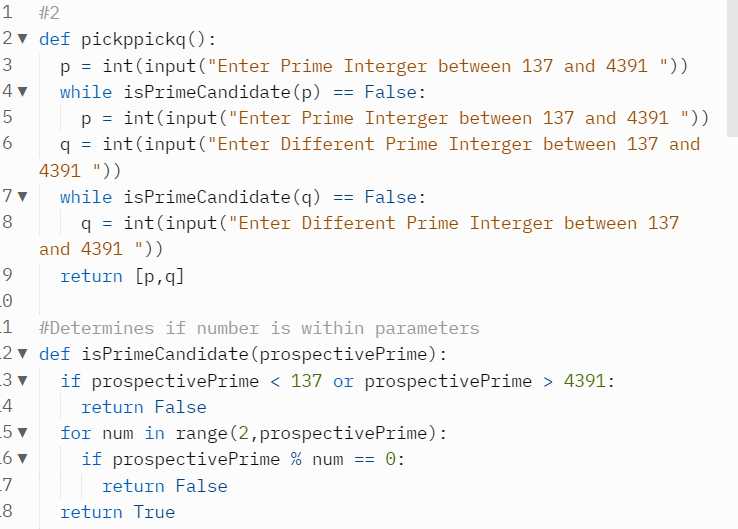
Morgan State University

RSA Project

Cryptography is the study of encryption, namely the ability to encode messages in such a way that it is very difficult to decode them without authorization. This can become a very involved process because of the increasing computing power that allows computers to run calculations quickly to figure out the code. RSA is an algorithm that encrypts messages using a public and private key. The public key is available to everyone, it allows encryption. While the private key is what allows for decryption. RSA works by using products of prime numbers, which are one-way functions. Multiplying prime numbers is trivial, it takes a negligible amount of computing power to do this. However, factoring large composites of prime numbers is extremely inefficient. The RSA function takes a string of plaintext, splits them into substrings of 3 length, converts these substrings into their numerical sum equivalent, and then puts this code to the power of the modulus number and then uses the modulus function on the product. After this tri number has been encrypted in this way, it is then converted back into plaintext by converting it to base 26 and getting the equivalent letter. This new encrypted text bears no resemblance to the original text and can only be decrypted using the private key, in basically the reverse order of the original function.

The functionality of the program as it exists currently:

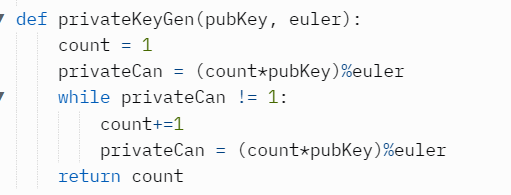
1. P and Q are requested from the user. The program makes sure that p is equal to or greater than 137 and less than or equal to 311.



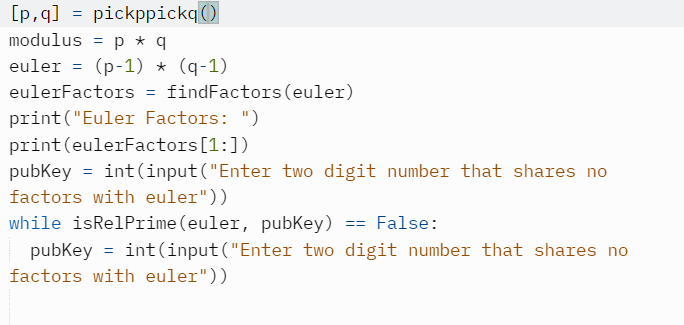
1. P and Q are multiplied creating the composite of the prime factors also known as the modulus.and the Euler Totient is generated by (P-1) multiplied with (Q-1)
2. The factors of the euler totient are calculated and displayed on screen, because the user must provide a two digit number that shares no factors with the euler totient this will serve as the public key, this is also known as being relatively prime.



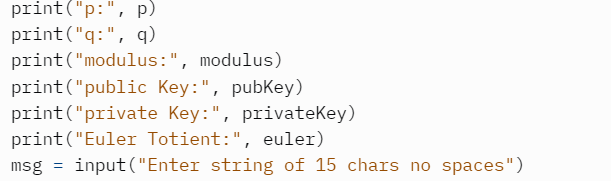
1. The private key is a number that when multiplied by the public key and divided by the modulus would give us back 1. So the private key is generated using a brute force method that multiplies the public key by i and checks the remainder when the product is divided by the modulus. When i satisfies this requirement it is returned as the private key.



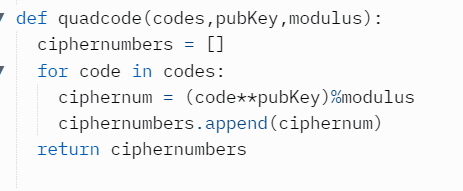
1. All the information is printed on screen, p, q, modulus, public key, private key, euler totient, to allow for checking the function for the correct calculations.



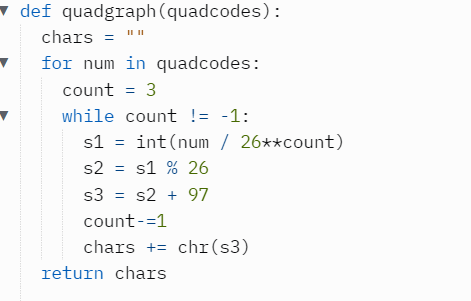
1. A plaintext message is requested from the user, the length must be divisible by 3, if not placeholders are added.



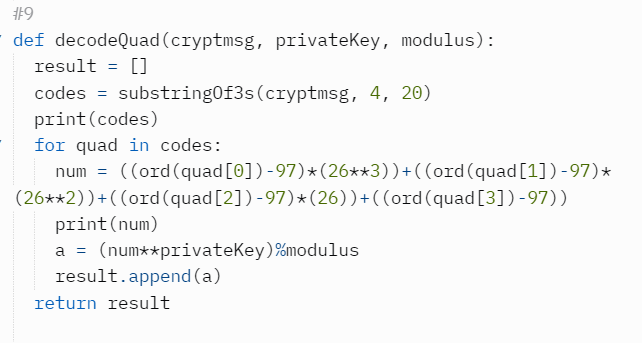
1. The message is split into substrings of 3 characters, these are translated into their number equivalent (ex: a = 0). And translated into base 26, the first character value multiplied by 26^2, second by 26, third by 1, these are all added to create the tricode value for each substring
2. Quadgraph codes are generated using the tricodes and multiplying them by the public key, this product is then divided by the modulus and the remainder becomes the quadcode.



1. Quad codes are made into quadgraphs by transforming the numbers out of base 26, this results in encrypted text in groups of 4 “arts”



1. To reverse this the quad decodes translates these quadcodes back into base 26, and multiplies each number by the private key, this product is divided by the modulus and the remainders make up the tricodes.



1. Decoding the tricodes is done by taking these tricodes out of base 26 and concatenating them into the plaintext message again.

