***Question 1***

For this question I wrote a python program that searches for first 3 smallest possible primes that 13 is their primitive roots.

A picture containing timeline

Description automatically generated

Therefore, 3 smallest possible prime numbers that 13 is their primitive root are 19, 31, 37.

***Question 2***

In this question first I had to factor out N to find p and q to calculate phi. Then I had to calculate private key using the phi, which calculated in previous step, for finding private key I had to use a modular multiplicative inverse algorithm with “gcd(e, phi) = 1” approach. Lastly, I have all information to be able to decrypt message or find out the original message, also to decrypt I had to find a fast modular exponentiation algorithm.

Text

Description automatically generated

After execution, results are as following:

***Question 3***

Since the question tells that every key and counter value are the same, it is easy to find encryption key and then decrypt cyphered text. It is needed to find the encryption key, which is the encrypt block, which after this I will call it “General Key”, in following diagram.

Diagram

Description automatically generated

since all the counter values and keys are same, we can generate easier diagram as follows:

Diagram

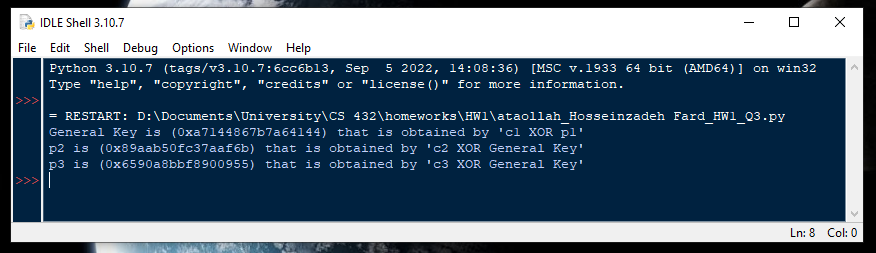
Description automatically generated

and now this diagram can be used both for encryption and decryption.

So, with using these equations first I found the General Key with doing xor on c1 and p1, then to find p2 and p3 I did xor General Key with c2 and General Key with c3. All the operation I did are as following diagram:

Diagram

Description automatically generated

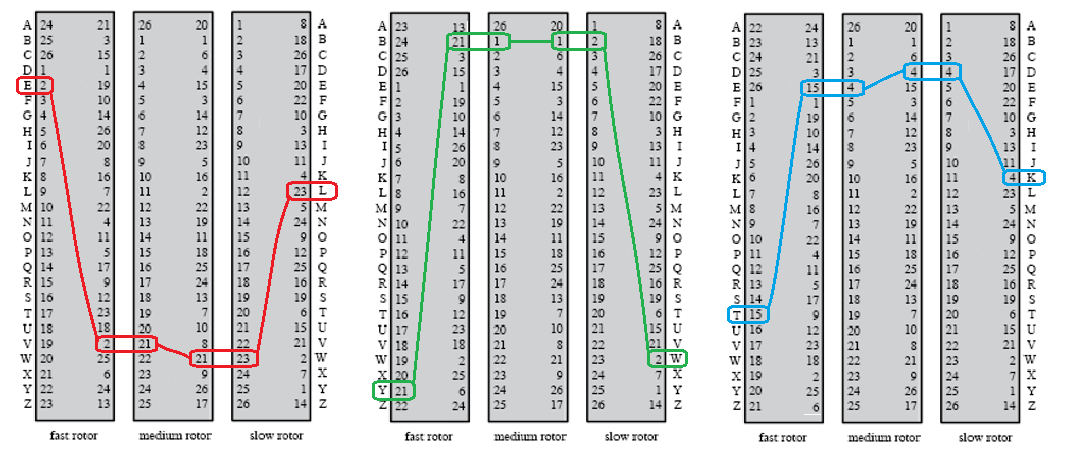
******

After execution, the results are as following:

89aab50fc37aaf6b 6590a8bbf8900955

***Question 4***

To encrypt “EYT” with 3 rotors, we should trace the indexes in each rotor to find position of next index. Moreover, after encryption of each letter, a stoke happens, that means left-most rotor shifts down, since we have only 3 letters, strokes will be limited to “fast rotor”, so for 1st letter no strokes, for 2nd letter 1 stroke, and for 3rd letter 2 strokes needed on the initial setting form.



Therefore, encryption of “EYT” with 3 rotors, with given initial settings, is “LWK”.