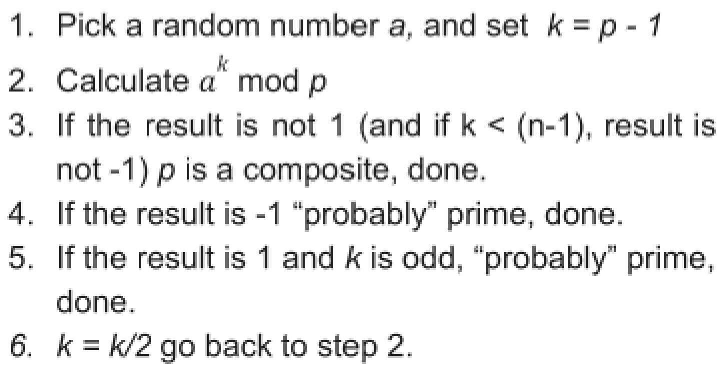
CENG418 Homework 1 Report
Arif Burak Demiray - 250201022

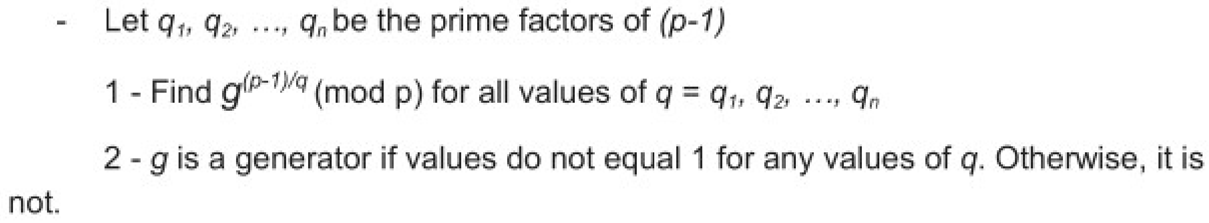
In this homework, we implemented very basic cipher system that is XOR cipher and we added CBC and DHKE for key distribution. I simply implemented two tests with given algorithms.

Primality Test



1. Pick a random number *a*, and set $k = p - 1$
2. Calculate a^k mod *p*
3. If the result is not 1 (and if k < (n-1), result is not -1) *p* is a composite, done.
4. If the result is -1 “probably” prime, done.
5. If the result is 1 and *k* is odd, “probably” prime, done.
6. $k = k/2$ go back to step 2.

Generator Test

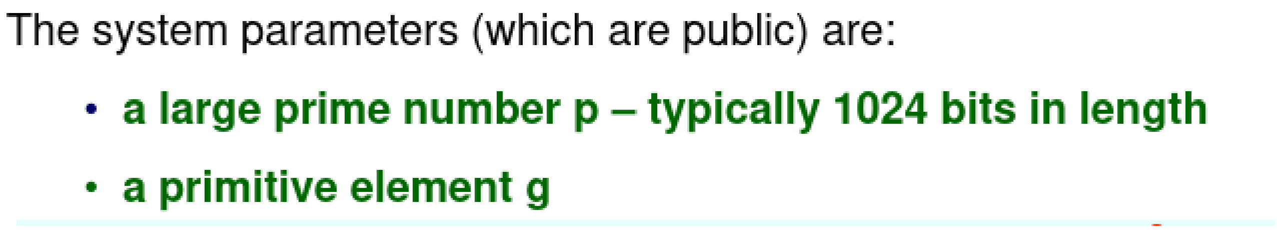


- Let $q_1, q_2, \ldots, q_n$ be the prime factors of *(p-1)*

1 - Find $g^{(p-1)/q}$ (mod p) for all values of $q = q_1, q_2, \ldots, q_n$

2 - *g* is a generator if values do not equal 1 for any values of *q*. Otherwise, it is not.

To test the given A and B, I checked them with GCD(G,A) and GCD(G,B)



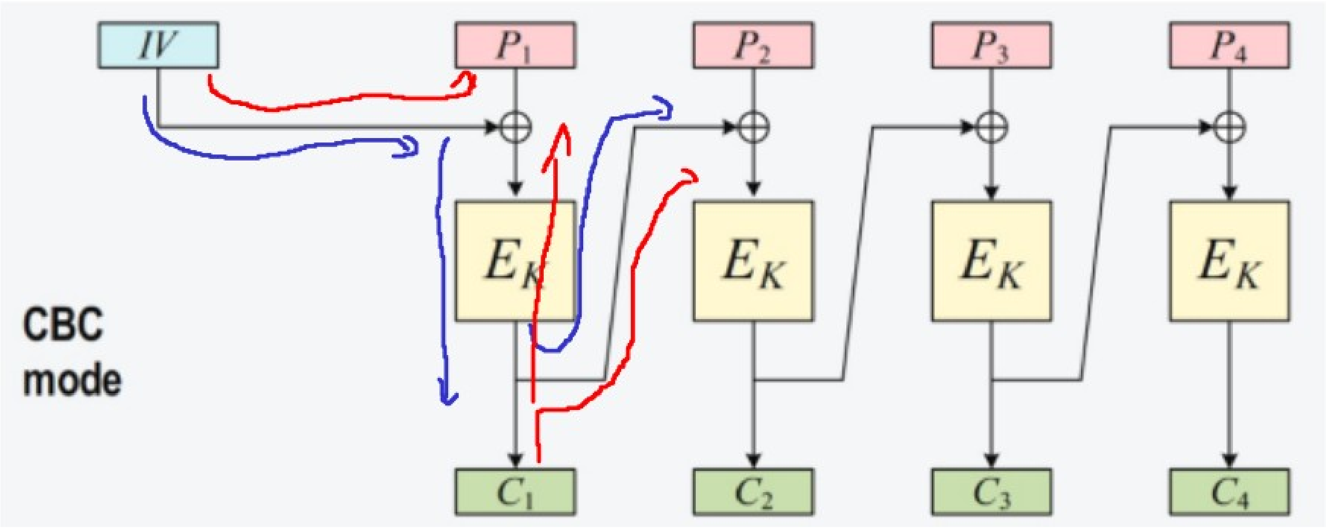
The system parameters (which are public) are:

- **a large prime number p – typically 1024 bits in length**
- **a primitive element g**

And I implemented prime factorization that dividing until not even, and then There can be at least one prime factor that would be less than sqrt of the number

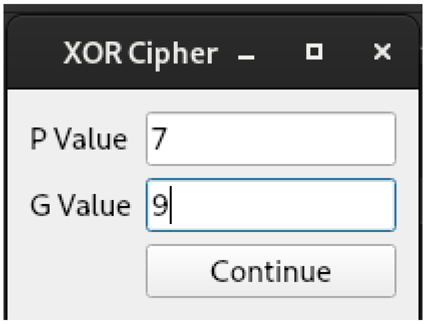
To find gcd of numbers, I implemented extended euclidean algorithm.

And to find modular exponinantion, take square of the number and took mod of it until power not 0



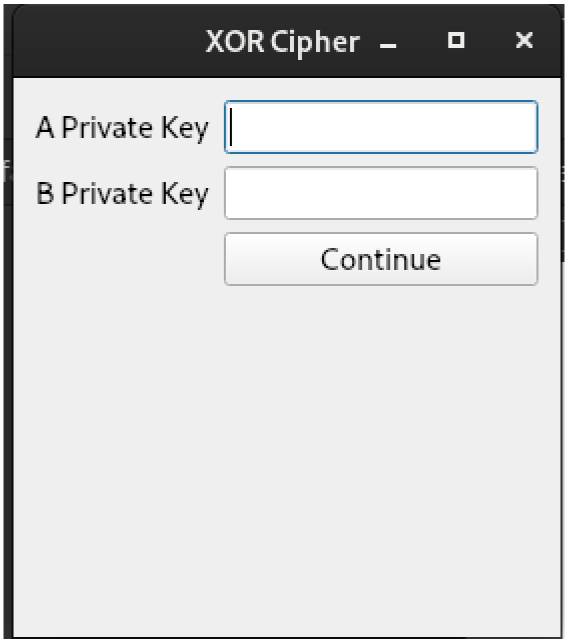
Also implemented cbc by given diagram. Encryption blue path, Decryption red path.

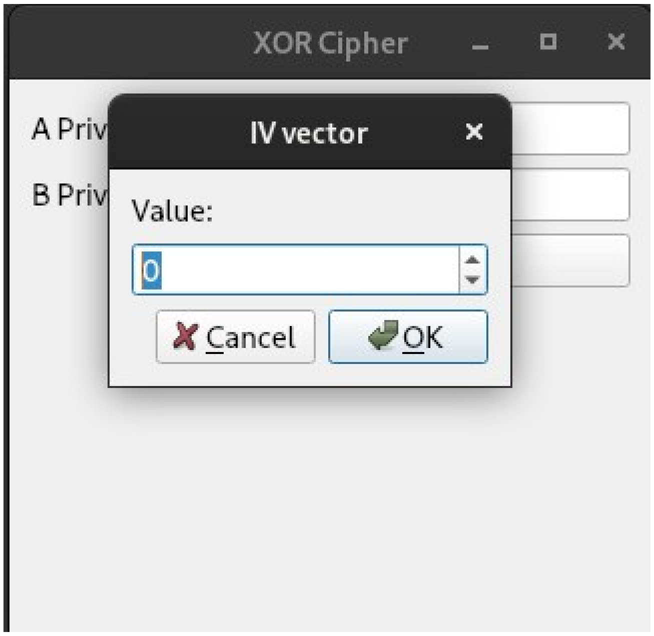
This homework absolutely needs a hashing algorithm to authenticate the sender and validate the message. Also, because publics are shared in channel, with man in the middle attack all things can be revealed. Also, it is XOR cipher it can easily decrypted because it is a two way function. I made a Cipher class which is responsible for encrypt-decrypt. Person class is for holding person specific informations. I used Python 3.8.6 and 3.10.2. I implemented UI in PyQt5.


XOR Cipher

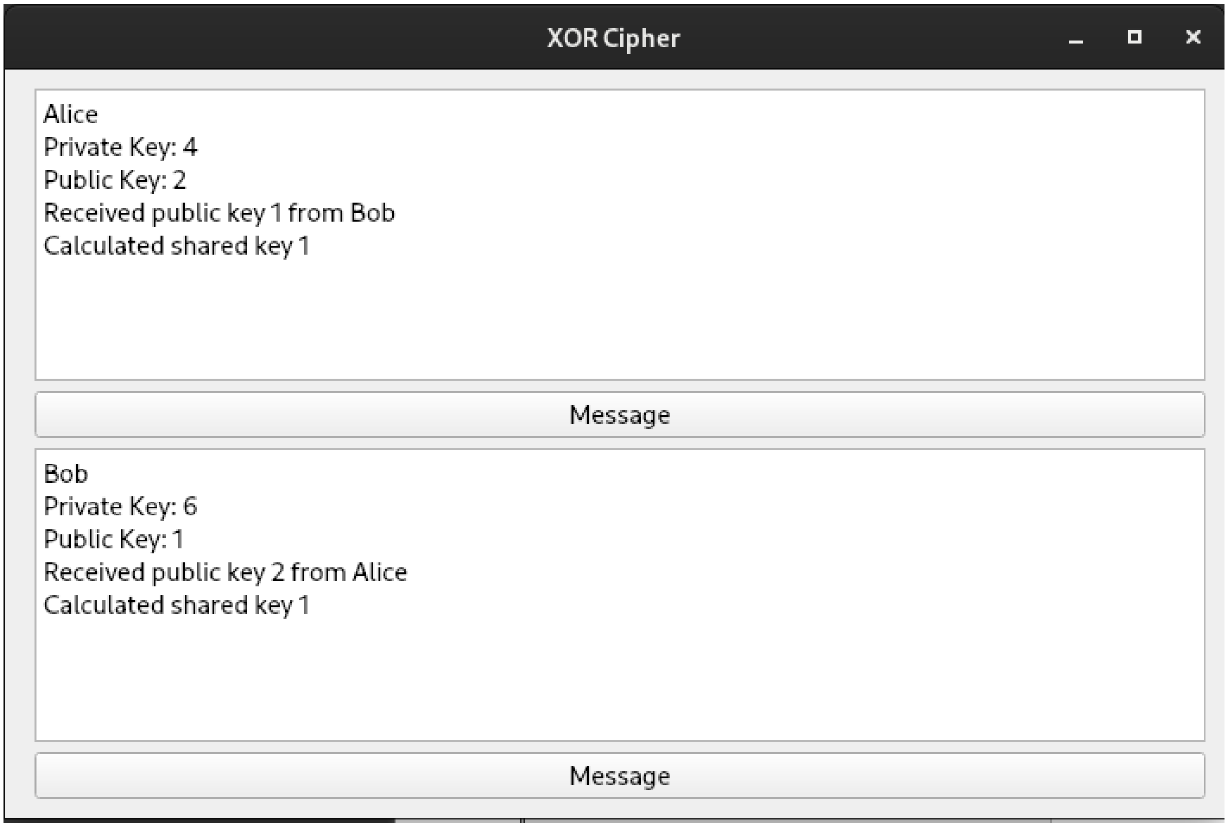
P Value 7

G Value 9


XOR Cipher
A Private Key
B Private Key
Continue

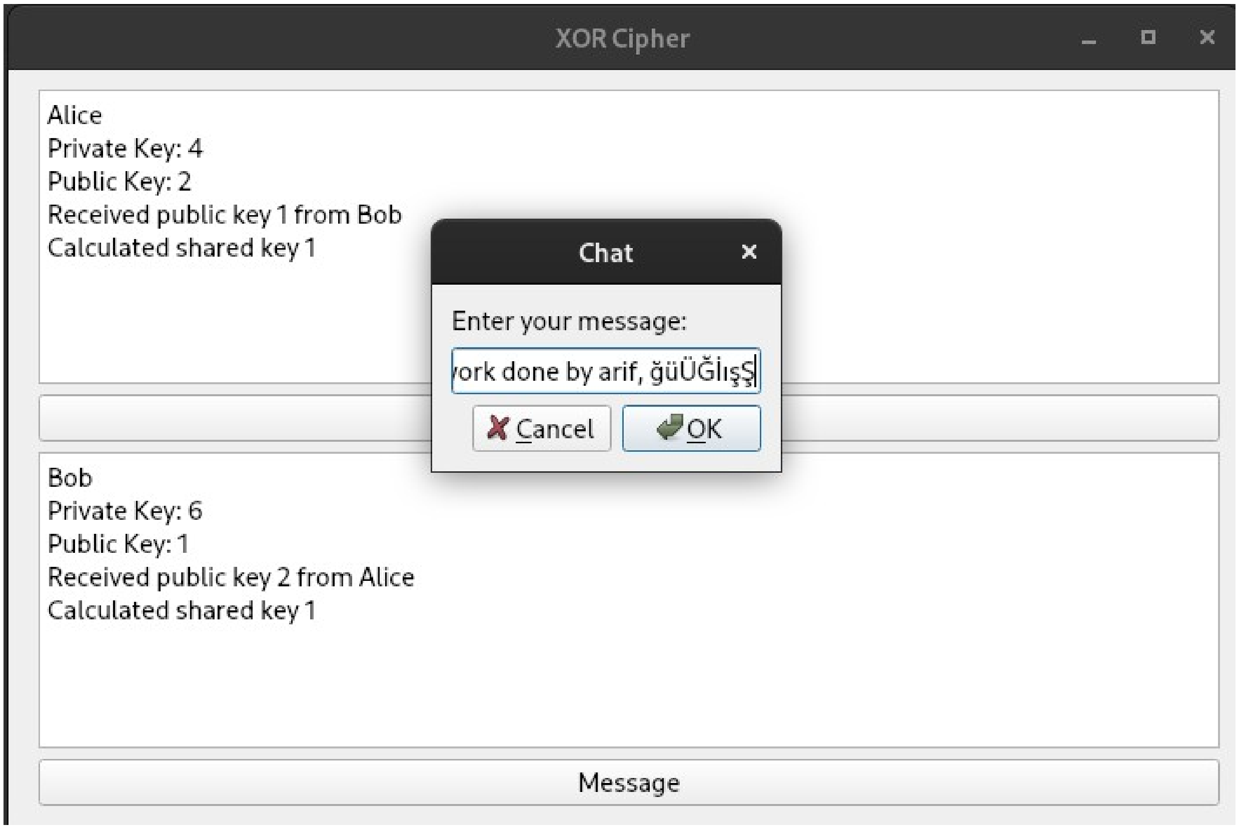

XOR Cipher
A Priv
B Priv
IV vector
Cancel
OK

Value: 0



```
Alice
Private Key: 4
Public Key: 2
Received public key 1 from Bob
Calculated shared key 1
```

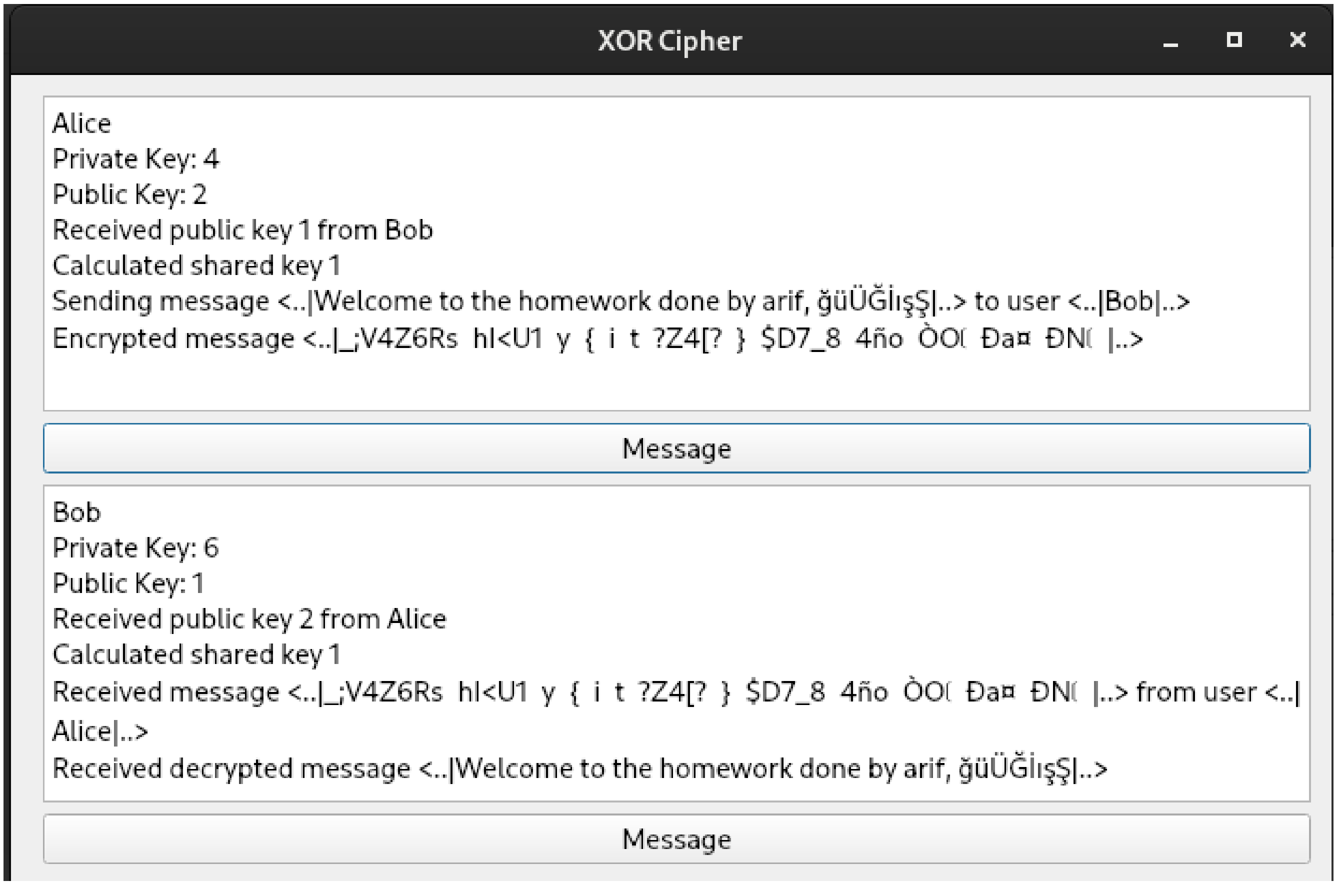
```
Bob
Private Key: 6
Public Key: 1
Received public key 2 from Alice
Calculated shared key 1
```



```
Alice
Private Key: 4
Public Key: 2
Received public key 1 from Bob
Calculated shared key 1
```

Enter your message: ork done by arif, ğüÜĞİışŞ

```
Bob
Private Key: 6
Public Key: 1
Received public key 2 from Alice
Calculated shared key 1
```



```
Alice
Private Key: 4
Public Key: 2
Received public key 1 from Bob
Calculated shared key 1
Sending message <..|Welcome to the homework done by arif, ğüÜĞİışŞ|..> to user <..|Bob|..>
Encrypted message <..|_;V4Z6Rs  hl<U1  y  {  i  t  ?Z4[?  }  $D7_8  4ño  ÒO(  Ða¤  ÐN(  |..>
```

```
Bob
Private Key: 6
Public Key: 1
Received public key 2 from Alice
Calculated shared key 1
Received message <..|_;V4Z6Rs  hl<U1  y  {  i  t  ?Z4[?  }  $D7_8  4ño  ÒO(  Ða¤  ÐN(  |..> from user <..|
Alice|..>
Received decrypted message <..|Welcome to the homework done by arif, ğüÜĞİışŞ|..>
```