ONLINE ELECTION UI

Problem Statement- In the post-pandemic world the election commission decides to hold elections online to maintain social distancing. Your task is to design and implement a secure protocol used for online elections that both maintains individual privacy and prevents cheating. The ideal protocol has, at the very least, these six requirements:
1. Only authorized voters can vote.
2. No one can vote more than once.
3. No one can determine for whom anyone else voted.
4. No one can duplicate anyone else’s vote. (This turns out to be the hardest requirement.)
5. No one can change anyone else’s vote without being discovered.
6. Every voter can make sure that his vote has been taken into account in the final tabulation.
Additionally, the government may have the following requirement:
7. Everyone knows who voted and who didn’t.

Theory - RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.
An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using the client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Generating Public Key :

Select two prime no's. Suppose P = 53 and Q = 59.

Now First part of the Public key : n = P*Q = 3127.

We also need a small exponent say e :

But e Must be

1. An integer.
2. Not be a factor of n.

$1 < e < \Phi(n)$ [$\Phi(n)$ is discussed below],

- Let us now consider it to be equal to 3.

Our Public Key is made of n and e

Generating Private Key :

We need to calculate $\Phi(n)$:
Such that $\Phi(n) = (P-1)(Q-1)$
so, $\Phi(n) = 3016$

Now calculate Private Key, d :
$d = (k*\Phi(n) + 1) / e$ for some integer k
For $k = 2$, value of d is 2011.

User Should Enter his name and private key from the user_priv.txt File.And Vote for the 1 of the Candidate. He can see the result by tapping ranking.

Link for user_priv.txt -
https://drive.google.com/file/d/1QKUrgYIBsqX1P4T3E2GxJuDgrUz2LZui/view?usp=sharing

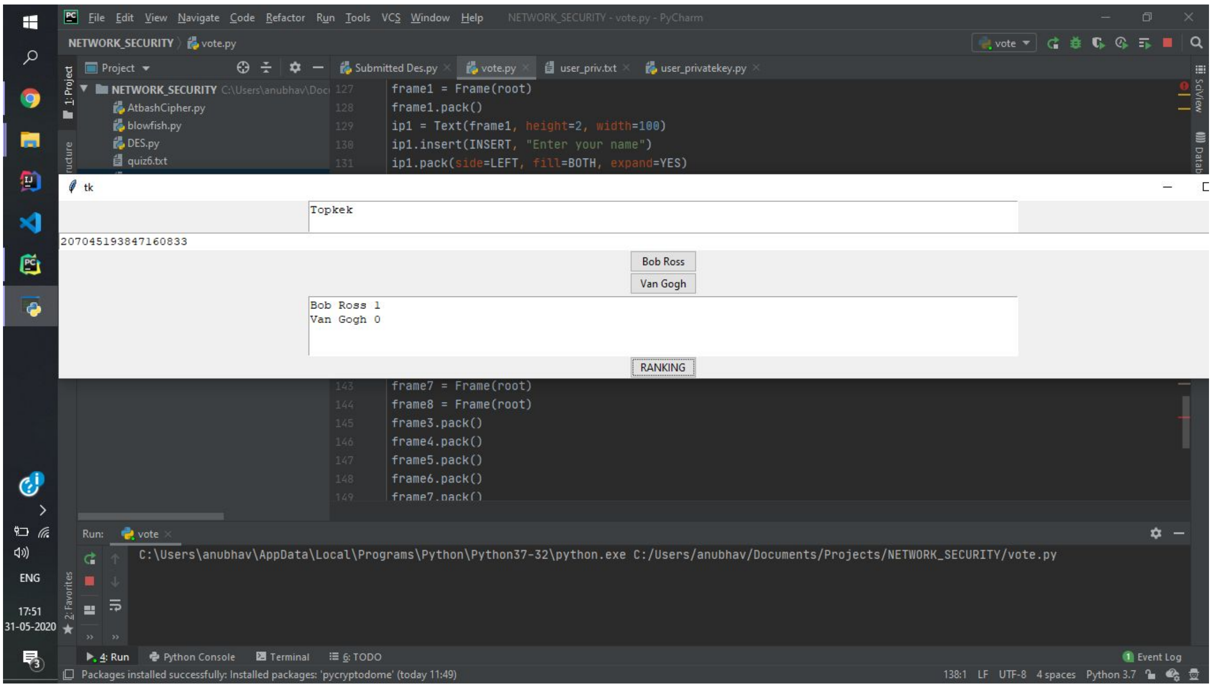
Link for generating user_priv.txt file -

https://drive.google.com/file/d/1RwEDKr0CUNppnCLHOSwNHvFAF-SM70tl/view?usp=sharing

Note- Here left values in the user_txt file correspond to private keys and right values correspond to uwu values which must be updated within the original code.

Original code link -
https://drive.google.com/file/d/1mkHLhWr_6DrYP7MFR4uZDPu7Tchc_PZI/view?usp=sharing

Screenshots-



```
frame1 = Frame(root)
frame1.pack()
ip1 = Text(frame1, height=2, width=100)
ip1.insert(INSERT, "Enter your name")
ip1.pack(side=LEFT, fill=BOTH, expand=YES)
```

```
Topkek
```

```
207045193847160833
```

```
Bob Ross 1
Van Gogh 0
```

```
frame7 = Frame(root)
frame8 = Frame(root)
frame3.pack()
frame4.pack()
frame5.pack()
frame6.pack()
frame7.pack()
```

```
C:\Users\anubhav\AppData\Local\Programs\Python\Python37-32\python.exe C:/Users/anubhav/Documents/Projects/NETWORK_SECURITY/vote.py
```

Packages installed successfully: Installed packages: 'pycryptodome' (today 11:49)

Conclusion - (1) Each voter signs his vote with his private key.

(2) Each voter encrypts his signed vote with the CTF's public key.

(3) Each voter sends his vote to the CTF.

(4) The CTF decrypts the votes, checks the signatures, tabulates the votes, and makes the results public.

(5) This protocol satisfies properties one and two: Only authorized voters can vote and no one can vote more than once.