

Note

The use of '\$' in the following inputs is to implicate command line inputs. It is not meant to be entered.

i.e.

Input:

```
$ foo
```

would imply the user entering 'foo' on the command line

Run make file

Input:

```
$ make
```

Output:

```
python3 -m venv venv
./venv/bin/pip install -r requirements.txt
Collecting cryptography
  Using cached cryptography-3.4.6-cp36-abi3-macosx_10_10_x86_64.whl (2.0 MB)
Collecting cffi>=1.12
  Using cached cffi-1.14.5-cp39-cp39-macosx_10_9_x86_64.whl (177 kB)
Collecting pycparser
  Using cached pycparser-2.20-py2.py3-none-any.whl (112 kB)
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.14.5 cryptography-3.4.6 pycparser-2.20
```

Run test

Input:

```
$ make run
```

Output:

```
./venv/bin/python3 unittesting.py
```

```
.....
```

```
-----  
Ran 8 tests in 0.514s
```

```
OK
```

```
./venv/bin/python3 registration_sim.py
```

```
This is a simulation of multiple users attempting to register and vote.
```

```
-----  
Please comment out the Sim() function as designated in Main for actual use.
```

```
As the valid voters are randomized, entering the same ID more than once may  
result in a user being "valid" one time and not another. Use in conjunction with  
an actual verification system to avoid this issue.
```

```
Press Enter to continue...
```

[Press Enter]

Output:

```
Loading ⋮
```

When finished loading

Output:

```
Finished!
```

```
Press Enter to see results...
```

[Press Enter]

Output:

```
-----
```

```
Attempt for ID: 18
```

```
-----
```

```
Successfully registered!
```

```
Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey objec
```

```
Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578cbcc70>
```

```
Signature: b'mqBbF5z0lNoo-QhVqk18KP8c-6QMbqFrNzy_dJ1VpwZXVcsVmL0mtuPykxIe6YzHp3Om2wR0UY7pXu7FJ-wP7HS61cnAx-fuRDS
```

```
Signature is correct: True
```

```
Attempting to vote for recipient 2
```

```
Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578cbcc70>
```

```
Recipient: recipient 2
Signature in transaction: b'mqBbF5z0lNoo-QhVqk18KP8c-6QMbqFrNzy_dJ1VpwZXVcsVmL0mtuPykxIe6YzHp30m2wR0UY7pXu7FJ-wP
Pending transactions: [<transaction.Transaction object at 0x7ff578cbc640>]
mining
Pending transactions: []

-----
Attempt for ID: 4
-----
Successfully registered!
Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c41af0>
Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41af0>
Signature: b'eypuv3Lip6AOA-AkulIPddi_SUtF6KHUE1IENB-_OKH8BNgWhW6aMs9WFJ7xY-J_Zdp2FH0oM5TK3l4imzzz3FMNaX-_oE1P_3Z
Signature is correct: True
Attempting to vote for recipient 5
Invalid candidate (only candidates 1 - 3 are registered), vote failed
Pending transactions: []
mining
Pending transactions: []

-----
Attempt for ID: 19
-----
Successfully registered!
Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c41c10>
Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41c10>
Signature: b'1-7mduevyNA2avQ8e0Lc3QfLh9uqC-5E8hNpoXgdQ5ndhjXHnZqOym2Hn9_m1CEPo7vNg4Jy8_m11d0Fs1A1VqXbiA5uXh7_JY_
Signature is correct: True
Attempting to vote for recipient 2
Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41c10>
Recipient: recipient 2
Signature in transaction: b'1-7mduevyNA2avQ8e0Lc3QfLh9uqC-5E8hNpoXgdQ5ndhjXHnZqOym2Hn9_m1CEPo7vNg4Jy8_m11d0Fs1A1VqXbiA5uXh7_JY_
Pending transactions: [<transaction.Transaction object at 0x7ff578ca93a0>]
mining
Pending transactions: []

-----
Attempt for ID: 18
-----
Voter ID already registered.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

-----
Attempt for ID: 12
-----
Successfully registered!
```

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c41ca0>
Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41ca0>
Signature: b'XX_ufh_GAzakfeB0b8ZLK6w8M5A1JwvZaVt-IpFJOV5ZRRnQ-CDho4-2LCudXupabeqMtWLTkKcQMzZ9cmZOMKdKLxvC7HzBzle'
Signature is correct: True
Attempting to vote for recipient 3
Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41ca0>
Recipient: recipient 3
Signature in transaction: b'XX_ufh_GAzakfeB0b8ZLK6w8M5A1JwvZaVt-IpFJOV5ZRRnQ-CDho4-2LCudXupabeqMtWLTkKcQMzZ9cmZOMKdKLxvC7HzBzle'
Pending transactions: [<transaction.Transaction object at 0x7ff578c41d60>]
mining
Pending transactions: []

Attempt for ID: 16

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 14

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 19

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 1

Successfully registered!
Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c41d90>
Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41d90>
Signature: b'y0u-8SNSwt0zIApsFezHrFE_kLYR0WGLQ2c7a_R6bifuTF79w5ZODItOwlFds2HP4ud6WBRl8gAz8FZF6BokcTPko3e9G30Ytrh'
Signature is correct: True
Attempting to vote for recipient 5
Invalid candidate (only candidates 1 - 3 are registered), vote failed
Pending transactions: []
mining

Pending transactions: []

Attempt for ID: 13

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c41fa0>

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41fa0>

Signature: b'QYoox9IDLXlVc9nguq9T05aQ-oVxb3GfyZ-IKk93uHnUesH9EHS_Hs_PayRvd4cfK3csYfTJeJRZCqgBi4Wdp1PJHzNz7kxbSkrF'

Signature is correct: True

Attempting to vote for recipient 2

Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c41fa0>

Recipient: recipient 2

Signature in transaction: b'QYoox9IDLXlVc9nguq9T05aQ-oVxb3GfyZ-IKk93uHnUesH9EHS_Hs_PayRvd4cfK3csYfTJeJRZCqgBi4Wdp1PJHzNz7kxbSkrF'

Pending transactions: [<transaction.Transaction object at 0x7ff578c41bb0>]

mining

Pending transactions: []

Attempt for ID: 14

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 11

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c44040>

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c44040>

Signature: b'Im-0uNugCZgiFCyKuL4mQxAbzMzdS94wdheNcstQz7Uv0aw0prs2bBGkqUMmOb2BFRE3uIT0ozT8U0vt3PvRz9-aeaW9xYHxjrF'

Signature is correct: True

Attempting to vote for recipient 5

Invalid candidate (only candidates 1 - 3 are registered), vote failed

Pending transactions: []

mining

Pending transactions: []

Attempt for ID: 5

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c44220>

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c44220>

Signature: b'UGV0to7pIPL5xo76oWNq4M1xXrQfhXdBIbrZ2m4XHCwwE03_x2DdFaW2ftf3ZsgEU74L33s23DZhue0dJh5ueI0SHSAAbc_wgkH'

Signature is correct: True

Attempting to vote for recipient 3
Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c44220>
Recipient: recipient 3
Signature in transaction: b'UGV0to7pIPL5xo76oWNq4M1xXrQfhXdBIbrZ2m4XHCwwE03_x2DdFaW2fTf3ZsgEU74L33s23DZhue0dJh5U
Pending transactions: [<transaction.Transaction object at 0x7ff578cbcb20>]
mining
Pending transactions: []

Attempt for ID: 6

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 1

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 9

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 19

Voter ID already registered.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 17

Invalid voter ID.
Private Key Object (Usually only shown to voter): 0
Public Key Object: 0
Don't Vote

Attempt for ID: 19

Voter ID already registered.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 2

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey objec

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c442b0>

Signature: b'F009FFzhVIPl6HUFYmm0sKJKm0HYLH2gmEvFuMo0x9KZJgpgxzEjF_OGkHMF9tBQYyX3h1dwGQiDQXMfUFe_ZhWDahhhxMMTHbR

Signature is correct: True

Attempting to vote for recipient 5

Invalid candidate (only candidates 1 - 3 are registered), vote failed

Pending transactions: []

mining

Pending transactions: []

Attempt for ID: 4

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 7

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey objec

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c443a0>

Signature: b'3skREei3TJ_l1zzFyNRHXC71rn3-BPGPhK0pqJDuzYPLyYjhQzXQowM-ff57Q4MMUCFQINPvU1eVDntNFRl6f8J0rAAWiy8e3C

Signature is correct: True

Attempting to vote for recipient 1

Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c443a0>

Recipient: recipient 1

Signature in transaction: b'3skREei3TJ_l1zzFyNRHXC71rn3-BPGPhK0pqJDuzYPLyYjhQzXQowM-ff57Q4MMUCFQINPvU1eVDntNFRl

Pending transactions: [<transaction.Transaction object at 0x7ff578c44490>]

mining

Pending transactions: []

Attempt for ID: 16

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 8

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c444c0>

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c444c0>

Signature: b'cUsJiJxBxDKARD7iuwQRKJwRl2fZpzXkrf88jP0VY3dZiKUYz7Lgf5IEfTU_DJyjdCGk4JvxlW6Par1HvCJP9oDMmxP00yYjcv'

Signature is correct: True

Attempting to vote for recipient 3

Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c444c0>

Recipient: recipient 3

Signature in transaction: b'cUsJiJxBxDKARD7iuwQRKJwRl2fZpzXkrf88jP0VY3dZiKUYz7Lgf5IEfTU_DJyjdCGk4JvxlW6Par1HvCJP9oDMmxP00yYjcv'

Pending transactions: [<transaction.Transaction object at 0x7ff578c445b0>]

mining

Pending transactions: []

Attempt for ID: 19

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 2

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 16

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 13

Voter ID already registered.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 9

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x7ff578c445e0>

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c445e0>

Signature: b'nftyS6T0QWsGbxhIZHbUL0PiKqEoskiJCVWRsYpeTjWMCIUg-0ETQHxLTerpp-pyy34drX_LFodq103M6EI7uRnpAUFEBYm7LCW

Signature is correct: True

Attempting to vote for recipient 2

Sender: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c445e0>

Recipient: recipient 2

Signature in transaction: b'nftyS6T0QWsGbxhIZHbUL0PiKqEoskiJCVWRsYpeTjWMCIUg-0ETQHxLTerpp-pyy34drX_LFodq103M6EI7

Pending transactions: [<transaction.Transaction object at 0x7ff578c446d0>]

mining

Pending transactions: []

Attempt for ID: 14

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 11

Voter ID already registered.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 7

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 13

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 15

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 19

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 7

Invalid voter ID.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 4

Voter ID already registered.

Private Key Object (Usually only shown to voter): 0

Public Key Object: 0

Don't Vote

Attempt for ID: 14

Successfully registered!

Private Key Object (Usually only shown to voter): <cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey objec

Public Key Object: <cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at 0x7ff578c44700>

Signature: b'NtrsKWmgE3wV6dfmKysJ2mrCcwmsJ0k_bOXvdXx020wGrBY2F2sXn0imQ6C_gNK0nANRr9z-rRqK1hq4mxmkeeLRASplCDDsXYI

Signature is correct: True

Attempting to vote for recipient 5

Invalid candidate (only candidates 1 - 3 are registered), vote failed

```
Pending transactions: []
```

```
mining
```

```
Pending transactions: []
```

```
-----  
Attempt for ID: 5  
-----
```

```
Voter ID already registered.
```

```
Private Key Object (Usually only shown to voter): 0
```

```
Public Key Object: 0
```

```
Don't Vote
```

```
-----  
Attempt for ID: 4  
-----
```

```
Voter ID already registered.
```

```
Private Key Object (Usually only shown to voter): 0
```

```
Public Key Object: 0
```

```
Don't Vote
```

Clean Up

Removes installed dependencies

Input:

```
$ make clean
```

Output:

```
rm -rf venv  
find . -type f -name '*.pyc' -delete
```

