

Part 1.

```
tholmquist@tholmquist:~/Downloads/434Lab3$ ./practiceRSA.py 128
public key is (17515351382659888200187863680492110124547454442684868576330351484
1939747514283,65537)
private key is (1751535138265988820018786368049211012454745444268486857633035148
41939747514283,35426513305895623546636285917384556167481178779721648772963325862
216905222613)
b'test,message'
36022907862226274534889187173
69085374925025299268252693170741024310080644631652350925923951435695807435447
b'test,message'
tholmquist@tholmquist:~/Downloads/434Lab3$
```

Part 2.

In order to decrypt the given message I first took the public key provided and fed it into this website <https://www.dcode.fr/prime-factors-decomposition>. I used the website to find the two prime numbers that were multiplied together to get the public key and then once I had those I fed them into my `make_key()` function from part one as `p1` and `p2`. Then I set `e` to be 65537, which was the number provided in the tuple for the public key and used those three numbers to create my own private key to match the public key to decrypt the message using the `make_key()` function from part 1. Then once I had the keys generated I ran the same decipher function from part one on the message and printed it to the screen using `.to_bytes(15)`. Then all I had to do was run the program `lab3-part2.py` and it printed out the key information and the message "b'congrats,passed'".