Phase 3 report

Requirements

Including authentication

Implementation details

For the prime numbers, I'll be using the following:

At first I tried to hard-code the bellow values for the public and private keys, but it was problematic and I ended up generating a new key for every session.

Client

p =
3136666666666666666666666666666666666666666666666666666666666666666666666666666666
6666666666666666666666666666666666666666666666666666666666666666666666666666666666
6666666666666666666666666666666666666666666666666666666666666666666666666666666666
6666666666666666666666666666666666666666666666666666666666666666313

q =
3130000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000011838110000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000313

which have been acquired from these links:

- https://primes.utm.edu/curios/page.php?number_id=10421
- https://primes.utm.edu/curios/page.php?number_id=162

Server

p =
2626417256821278393346689388471903317983111453336167929583728384248571567750072271
0245492814818316782321153464194329979596230957987468291356860865095919337082447486
3282145037585560618568778906679404993323367715662527874977471424467472818616772123
8664217142320292848284760221139877817176584863695983931661930322854971538374547662
80540159

q =
1357911131517193133353739515355575971737577799193959799111113115117119131133135137
139151153155157159171173175177179191193195197199311313315317319331333353373393513

5335535735937137337537737939139339539739951151351551751953153353553753955155355555
7559571573575577579591593595597599711713715717719731733735737739751753755757759771

which have been acquired from these links:

- https://primes.utm.edu/curios/page.php?number_id=3183
- https://primes.utm.edu/curios/page.php?number_id=10319

For the cryptographically secure random number generation, I'm using python's secrets library.

Diffie Hellman

The vaules were hardcoded and chosen from the following website:
https://www.ietf.org/rfc/rfc3526.txt

2048-bit MODP Group

This group is assigned id 14.

This prime is: 2^2048 - 2^1984 - 1 + 2^64 * { [2^1918 pi] + 124476 }

Its hexadecimal value is:

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D
670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B
E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9
DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
15728E5A 8AACAA68 FFFFFFFF FFFFFFFF
```

The generator is: 2.

Assignment details

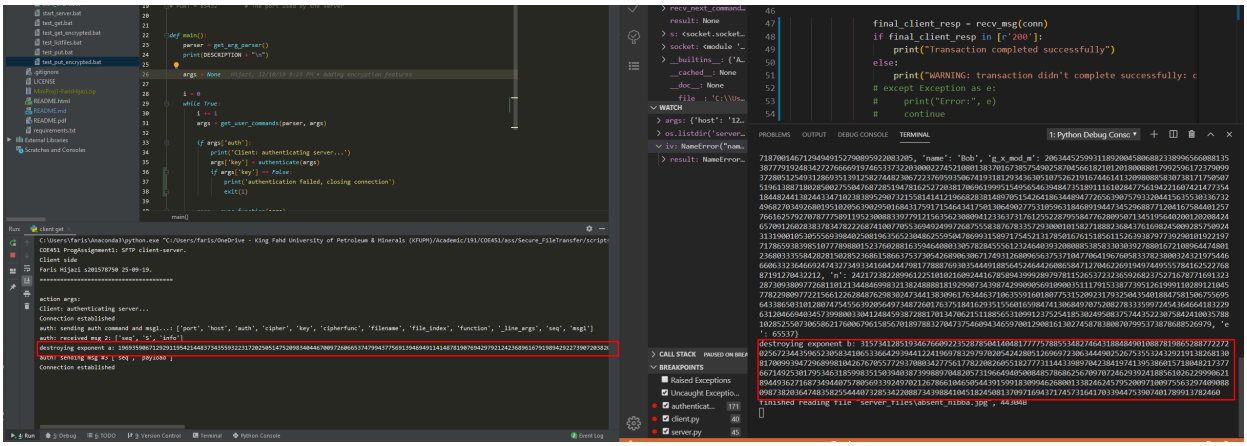
The code changes made for phase 3 can be found on GitHub, the branch phase3-auth.
You can see the code changes made on this page.

The added code was mainly the authentication.py file

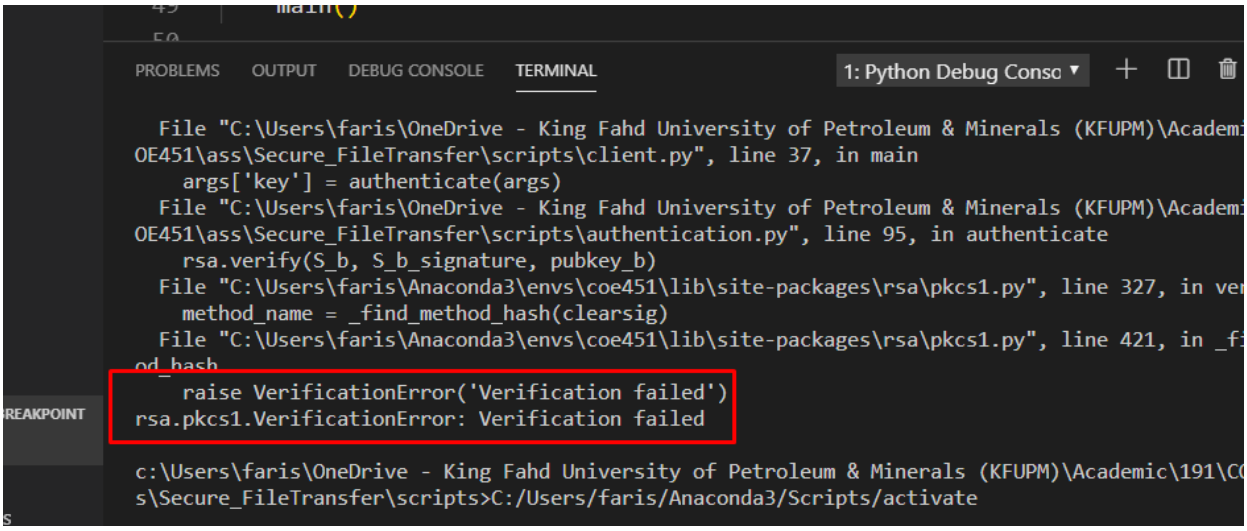
Tests and screenshots

to perform test1 and test2, you can pass the `--test=1` or `--test=2` arguments on the client's side.

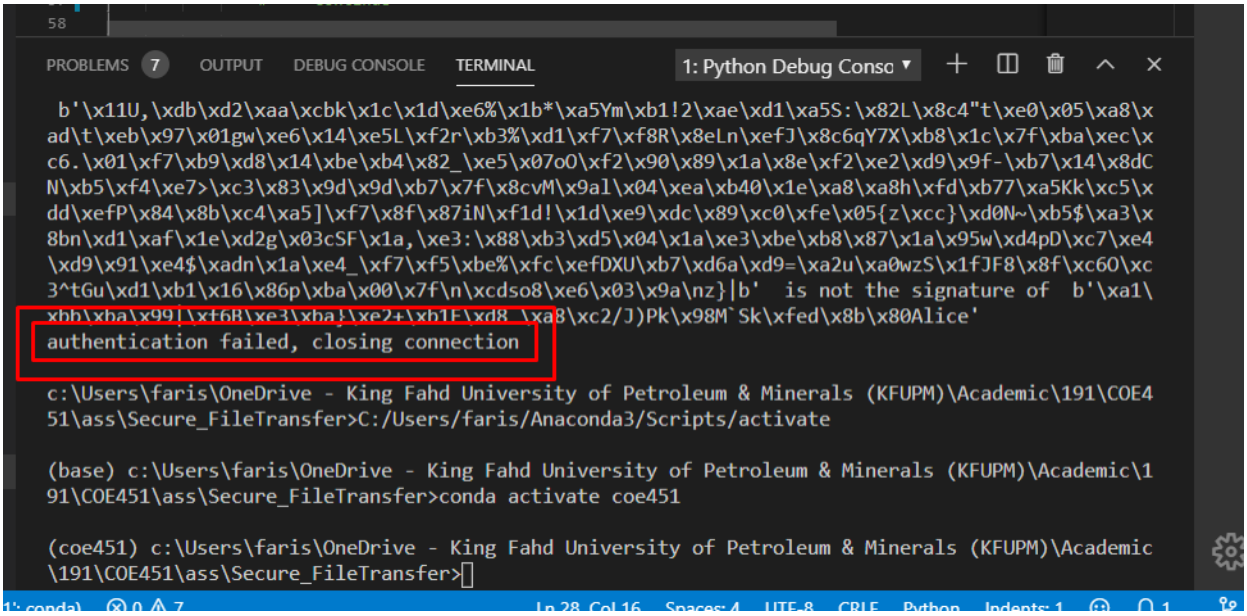
Showing exponent



Bad key for bob (failed authentication)



testcase3 TrudyPosingAsAlice


58
PROBLEMS 7
OUTPUT
DEBUG CONSOLE
TERMINAL
1: Python Debug Conso
b'\x11U,\xdb\xd2\xaa\xcbk\x1c\x1d\xe6%\x1b*\xa5Ym\xb1!2\xae\xd1\xa5S:\x82L\x8c4"t\xe0\x05\xa8\x
ad\t\xeb\x97\x01gw\xe6\x14\xe5L\xf2r\xb3%\xd1\xf7\xf8R\x8eLn\xefJ\x8c6qY7X\xb8\x1c\x7f\xba\xec\x
c6.\x01\xf7\xb9\xd8\x14\xbe\xb4\x82_\xe5\x07oO\xf2\x90\x89\x1a\x8e\xf2\xe2\xd9\x9f-\xb7\x14\x8dC
N\xb5\xf4\xe7>\xc3\x83\x9d\x9d\xb7\x7f\x8cvM\x9al\x04\xea\xb40\x1e\xa8\xa8h\xfd\xb77\xa5Kk\xc5\x
dd\xefP\x84\x8b\xc4\xa5]\xf7\x8f\x87iN\xf1d!\x1d\xe9\xdc\x89\xc0\xfe\x05{z\xcc}\xd0N~\xb5$\xa3\x
8bn\xd1\xaf\x1e\xd2g\x03cSF\x1a,\xe3:\x88\xb3\xd5\x04\x1a\xe3\xbe\xb8\x87\x1a\x95w\xd4pD\xc7\xe4
\xd9\x91\xe4$\xadn\x1a\xe4_\xf7\xf5\xbe%\xfc\xefDXU\xb7\xd6a\xd9=\xa2u\xa0wzS\x1fJF8\x8f\xc6O\xc
3^tGu\xd1\xb1\x16\x86p\xba\x00\x7f\n\xcdso8\xe6\x03\x9a\nz}|b' is not the signature of b'\xa1\
xbb\xba\x99|\xf6R\xe3\xba}\xe2+\xb1F\xd8 \xa8\xc2/J)Pk\x98M`Sk\xfed\x8b\x80Alice'
authentication failed, closing connection
c:\Users\faris\OneDrive - King Fahd University of Petroleum & Minerals (KFUPM)\Academic\191\COE4
51\ass\Secure_FileTransfer>C:/Users/faris/Anaconda3/Scripts/activate
(base) c:\Users\faris\OneDrive - King Fahd University of Petroleum & Minerals (KFUPM)\Academic\1
91\COE451\ass\Secure_FileTransfer>conda activate coe451
(coe451) c:\Users\faris\OneDrive - King Fahd University of Petroleum & Minerals (KFUPM)\Academic
\191\COE451\ass\Secure_FileTransfer>