Homework 19, due October 20

(1) (a) (Page 193, problem 10) The exponents $e = 1$ and $e = 2$ should not be used in RSA. Why?

(b) (Page 193, problem 8) In order to increase security, Bob chooses n and two encryption exponents e_1, e_2. He asks Alice to encrypt her message m to him by first computing $c_1 \equiv m^{e_1} \pmod{n}$ and then encrypting c_1 to get $c_2 \equiv c_1^{e_2} \pmod{n}$. Alice then sends c_2 to Bob. Does this double encryption increase security over single encryption? Why or why not?

(2) Use the Fermat factorization method to decrypt.

```
c = 71582563460749316228031805686158989313492125191803635955104 99\
3945856531643361869650804419086652922049711054772891912306619325 3\
60528766398068836270349244 36,
(n,e) = (13407807929942597099574024998205846128120955988962922985\
48545924680147453708091573208613509123248935945157972778932936509\
18329641402370302455953081207542 27, 65537).
```

(3) A message, with corresponding ciphertext

```
c = 27323511547402228211346661525937327912891027377849543661139 1\
48281068460497102133361755180097355395227950936088582719808910 70\
81752517053854233268,
```

was encrypted with the public key

```
(n,e) = (77091027375829461525275245559332514392988124609273729603\
22410154686401572970611709262810088591805749309232637320702695246\
68336515343198285987851, 17).
```

Decrypt. If $n = pq$, can you factor $p - 1$ or $q - 1$?