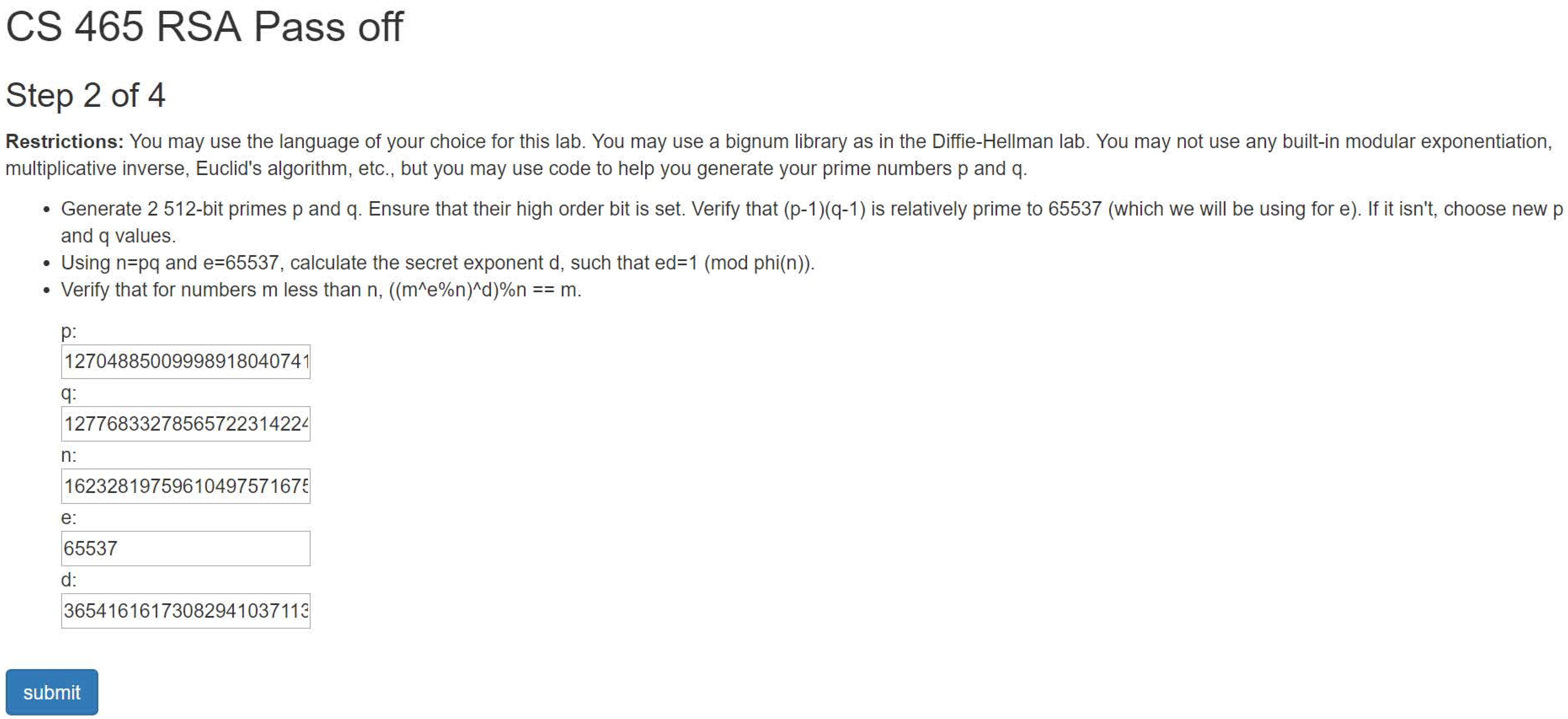


CS 465 RSA Pass off

Step 2 of 4

Restrictions: You may use the language of your choice for this lab. You may use a bignum library as in the Diffie-Hellman lab. You may not use any built-in modular exponentiation, multiplicative inverse, Euclid's algorithm, etc., but you may use code to help you generate your prime numbers p and q.

- Generate 2 512-bit primes p and q. Ensure that their high order bit is set. Verify that (p-1)(q-1) is relatively prime to 65537 (which we will be using for e). If it isn't, choose new p and q values.
- Using n=pq and e=65537, calculate the secret exponent d, such that ed=1 (mod phi(n)).
- Verify that for numbers m less than n, ((m^e%n)^d)%n == m.

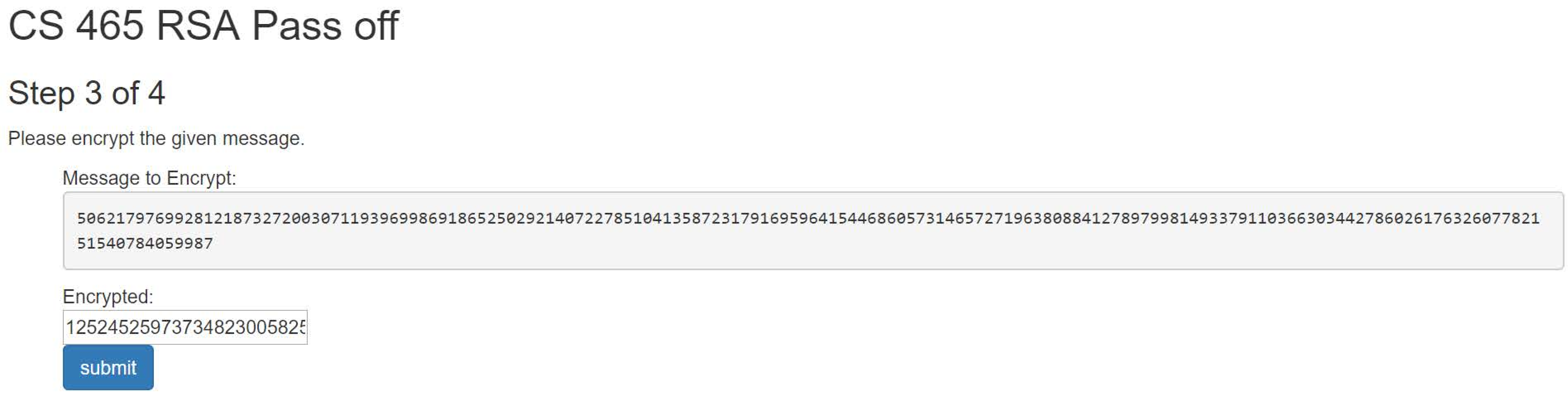
p:
12704885009998918040741

q:
12776833278565722314224

n:
16232819759610497571675

e:
65537

d:
36541616173082941037113



CS 465 RSA Pass off

Step 3 of 4

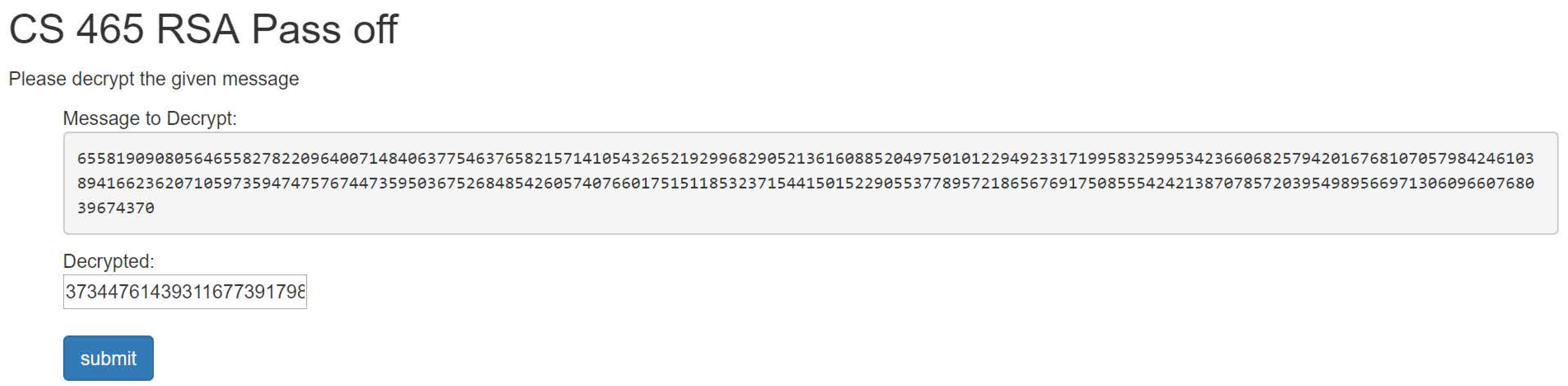
Please encrypt the given message.

Message to Encrypt:

```
506217976992812187327200307119396998691865250292140722785104135872317916959641544686057314657271963808841278979981493379110366303442786026176326077821
51540784059987
```

Encrypted:

12524525973734823005825



CS 465 RSA Pass off

Please decrypt the given message

Message to Decrypt:

```
655819090805646558278220964007148406377546376582157141054326521929968290521361608852049750101229492331719958325995342366068257942016768107057984246103
894166236207105973594747576744735950367526848542605740766017515118532371544150152290553778957218656769175085554242138707857203954989566971306096607680
39674370
```

Decrypted:

37344761439311677391798

CS 465 RSA Pass off

Congratulations you have completed the RSA lab!