- recall your choice of P,q, and e: P=* q=* e=* *use missy's list

  (all of them have been checked and are valid)

  let's find the modulus, N:

  recall, N = P * q

  N: □

  correct responce → . - -

  Correct!

  wrong responce → . . .

  in this step you must multiply P and q

- now it's time for encryption:

  recall, your public key = (N,e)

  with your numbers its : (N, e)

  you have picked the message message to encrypt.

  to compute the ciphertext, we will use the following formula: $C = m^e \bmod N$

  C = □

  Correct!

  first compute m^e

  C will be the remainder of the division m^e/N

- Now that encryption is done. Let's see how Bob would decrypt the message:

  To find secret exponent d, we must first make sure

ϕ is correct. recall $\phi = (p-1)(q-1)$

ϕ: ______

correct!

ϕ is the result of multiplying $(p-1)$ & $(q-1)$ make sure your calculations are correct!

- now that we know ϕ, let's find the secret exponent, d
  recall $1 < d < \phi$ & $ed = 1 \bmod \phi$

d = ______

correct!

we are looking for a d such that ϕ divides $ed - 1$.

- last step! let's decrypt!
  to decrypt the ciphertext into plain text, we use the following formula: $m' = c^d \bmod N$

m': ______

correct!
you've learned the RSA cryptosystem!

First calculate c^d.
then find the remainder of the division: $\frac{c^d}{N}$