26. RSA- Really Simple Algorithm

For this question we will be attempting to go through the entire process of decoding a RSA cipher. We will be using very small primes, but in reality very large primes are often used to prevent the modulus N from being factored and thus having the cipher broken.

In decoding RSA, you are usually given the public key and the modulus N. For this question our N will be 35.

a. Factor the modulus N into its primes. (25 points)

b. Calculate phi(N) (also known as Euler's totient). (75 points)

The public key can be any number, but it must be coprime with phi(N).

c. Which number can be used as e in this scenario? (25 points)
   i. 48
   ii. 99
   iii. 72
   iv. 25

We will select 29 as our public key for this scenario. By factoring N and calculating phi(N), we can now calculate our private key, d. The private key is defined as d*e=1 mod phi(N).

d. Calculate the private key, d. (150 points)

Now that we have our private key, we are ready to decode our message. We will stick with a 26 letter alphabet for this question. The message we are trying to decode is
12 # 08 # 21 # 09 # 23 # 24 # 23 # 07 # 00 # 17 # 08 # 12 # 00 # 33 # 16 # 09 # 17 # 00 # 13
(Normally RSA is not expressed like this, however this will simplify the calculations)
The equation of the decryption is (ciphertext)^{d} mod N.

e. Please decode the message and express the decoded message as numbers and not letters. For example if your output is 0, please express your plaintext as A, if your output is B, please express it as 1, and so forth. The standard two error rule applies here. (300 points)

Congratulations! You have (hopefully) decoded the contents of the RSA cipher. Here is a bonus question with much larger numbers. I do not recommend using the same process described earlier.
You received the ciphertext 13824. You know that the public key is 3 and the modulus N is 26167. Luckily you managed to already factor 26167 into 137 and 191. Please decrypt the sent message. The answer should be composed of one letter. (200 points)