RSA2

For this challenge, we can see that m and n are the same and e is different for both messages. Thus, we can do a common modulus attack.

Consider the following:

Modulus arithmetic rules:

1. (A * B) mod C = (A mod C * B mod C) mod C

2. (A ^ B) mod C = ((A mod C) ^ B) mod C

The following algorithm can be manipulated to show that it will be useful when trying to get the flag:

((c1^u mod n)*(c2^v mod n)) mod n

= (((m^e1 mod n)^u mod n)*((m^e2 mod n)^v mod n)) mod n.

= ((m^(e1*u) mod n)*(m^(e2*v) mod n)) mod n.   by 2.

= m^(e1*u+e2*v) mod n.   by 1.

If we make e1*u+e2*v = 1, we will get m^1 mod n = m mod n = m, which will give us the flag.

Consider Bézout's identity: ax + by = gcd(a,b). When a and b are coprime (gcd(a,b) = 1), x is the modular multiplicative inverse of a modulo b. This can be calculated with gmpy2.invert(a,b). Therefore, u can be calculated through:

u = gmpy2.invert(e1, e2)

Now, from (e1*u)+(e2*v) = 1, we can rearrange to solve for v:

v = (1 - (e1*u))/e2

Now, we have u and v. Thus, we just need to plug them into the equation m = ((c1^u mod n)*(c2^v mod n)) mod n to get back m. After that, we can convert the integer m back to ascii and get the flag. Thus, this challenge is solved.