Modular Binomials

1 Disclosure

I didn't solve this Challenge on my own completely. I got idea until binomial expansion and stuck there. I looked online and found this article. I understood the solution and now writing it in more detail.

2 Write-up

First things first, By Symmetry, We can interchange the c_1 and $(2^p + 3^q)$. In the expansion of $(x+y)^n$, We can ignore all terms except first and last. Because all the terms except first and last contain the product of x and y, and Since $N = p * q$, Their contribution to modulo N is 0. Combining all properties, we get following equations.

$$((2p)^{e_1} + (3q)^{e_1}) \equiv c_1 mod N \tag{1}$$

$$((5p)^{e_2} + (7q)^{e_2}) \equiv c_2 mod N \tag{2}$$

By compatibility with exponentiation, And using above property again (i.e., Ignoring middle terms), we get,

$$((2p)^{e_1 e_2} + (3q)^{e_1 e_2}) \equiv c_1^{e_2} mod N \tag{3}$$

$$((5p)^{e_1 e_2} + (7q)^{e_1 e_2}) \equiv c_2^{e_1} mod N \tag{4}$$

Let's define few variables for convenience. $a = 2^{e_1 e_2}$, $b = 3^{e_1 e_2}$, $x = c1^{e_2}$, $c = 5^{e_1 e_2}$, $d = 7^{e_1 e_2}$, $y = c_2^{e_1}$. Note that,

$$x = (ap^{e_1 e_2} + bq^{e_1 e_2}) mod N$$

$$y = (cp^{e_1 e_2} + dq^{e_1 e_2}) mod N$$

$$p = gcd(dx - by, N)$$

$$q = gcd(ay - cx, N)$$