MODULAR BINOMIALS (80pts)

Rearrange the following equations to get the primes p,q

$$N = p \cdot q$$
$$c_1 = (2 \cdot p + 3 \cdot q)^{e_1} \mathrm{mod} N$$
$$c_2 = (5 \cdot p + 7 \cdot q)^{e_2} \mathrm{mod} N$$

Multiply both of the equations by each other to get similar equations

C1^e2 = (2p + 3q)(^e1^e2) modN

C2^e1 = (5p + 7q) (^e2^e1) modN

Now multiply equation C1 by 5 and C2 by 2, in order to get the same p value , u can also multiply to get same q value here but I will use p

Remember to use Power Rule: a^b x c^b = (a x c)^b

So we multiply by 5^(e1 ^ e2) and 2^(e1 ^ e2)

Equation1 = (10p + 15q)^e1^e2 modN = 5^e1^e2 x c1^e2

Equation2 = (10p + 14q)^e1^e2 modN = 2^e2^e1 x c2^e1

Now subtract these equations to get q(^e1^e2) mod N

We know that from earlier N = p x q

And we know the difference between equation 1 and equation2 is a multiple of q

And that q is a common divisor for both equations (n =p x q) and the difference of equation 1 and 2 (eqn_1 - eqn_2)

Therefore q is a factor of the difference of equation 1 and 2 and its also a factor of N

So the greatest common divisor of both (eqn_1 - eqn_2) and N will give you q

Now all we have to is get the already provided values from the txt file and insert it all into a python script….