**1. Overview**

I decided to use python to do the computations

Part1: p=11 and q=23

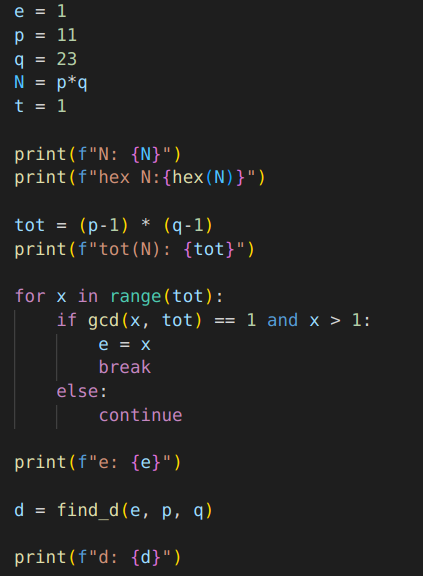
1. N = 220

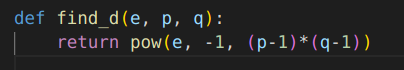
2. N in hex = fd

3. totient of N is defined as lcm(p-1, q-1) which is just (p-1)\*(q-1) since p and q are prime, tot(N)= 220

4. find e such that 1 < e < tot(N), use a simple while loop to find suitable e = 3:

5. find d such that ed = 1 (mod tot(N)) this implies d = e ^ -1(mod tot(N)), use the python pow function: pow(e, -1, (p-1)\*(q-1))







6. Bob sent picked 1 < x < N and encrypts it with (N, e) then sends y = 00001111 in binary, use our d from the previous question to find x

since we know d, y and N:

x = y ^ d mod N = 159

7. Alice sent the encrypted message 10100011 in binary to Bob, Bob’s modulus, N is f7 in hex and his exponent e, is 7. Find Alice’s original message

since f7 is small we can just loop through all possible numbers p and q until we find two for which p\*q = N. Those will be our prime numbers from which we can do the decryption

we find p = 13 and q = 19 with which we can get d = 31 using which we can compute x = y ^ d mod N = 10100011 ^ 31 mod f7 = 201

