13. Write a high level code for set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

CODE ::

from math import gcd

n = int(input("ENTER N VALUE = "))

e = int(input("ENTER E VALUE = "))

blocks = [877, 2067, 1180, 3317, 1608]

block\_with\_common\_factor = None

for block in blocks:

if gcd(block, n) > 1:

block\_with\_common\_factor = block

break

p = gcd(block\_with\_common\_factor, n)

q = n // p

phi\_n = (p - 1) \* (q - 1)

d = pow(e, -1, phi\_n)

decrypted\_blocks = [pow(block, d, n) for block in blocks]

print("Private key: ({}, {})".format(d, n))

print("Decrypted blocks:", decrypted\_blocks)

OUTPUT ::

