#Andrew candelaresi
#Algorithms HW2
#104005676
#On my honor, as a University of Colorado at Boulder student, I have neither #given nor recieved unauthorized assitance on this work.

1. to multiply an m bit number by an n bit number will take m*n time since the algorithm for multiplication is in O(n^2)

2. gcd(770, 546)
   a. factors 770: 1, 2, 5, 7, 10, 11, 14, 22, 35, 55, 70, 77, 110, 154, 385, 770
      factors 546: 1, 2, 3, 6, 7, 13, 14, 21, 26, 39, 42, 78, 91, 182,273, 546
      gcd(770, 546) = 14
   b. Euclid(770, 546)
      546!= 0
      Euclid(546, 770 mod 546) = Euclid(546, 224)
         224 != 0
         Euclid (224, 546 mod 224) =Euclid(224, 98)
            98 != 0
            Euclid (98, 224 mod 98) = Euclid(98, 28)
               28!=0
               Euclid(28, 98 mod 28) = Euclid(28, 14)
                  14!=0
                  Euclid(14, 28 mod 14) = Euclid(14, 0)
                     0==0
                     return 14
   c. ext-Euclid(770,546)
      546!= 0
      ext-Euclid(546, 770 mod 546) = ext-Euclid(546, 224)
         224 != 0
         ext-Euclid (224, 546 mod 224) =ext-Euclid(224, 98)
            98 != 0
            ext-Euclid (98, 224 mod 98) = ext-Euclid(98, 28)
               28!=0
               ext-Euclid(28, 98 mod 28) = ext-Euclid(28, 14)
                  14!=0
                  ext-Euclid(14, 28 mod 14) = ext-Euclid(14, 0)
                     0==0
                     return (1,0,14)
      (1,0,14)
      a = 28 b=14 (0,1,14)
      a = 98 b=28 (1,-3,14)
      a=224 b=98 (-3,7,14)
      a=546 b=224 (7,-17,14)
      a=770 b=546 (-17,24,14)

   gcd(770,546) = 14 = 770*(-17) + 546*24

3. 7^7293(mod 342)
   modexp(7,7293,342)
      7293 != 0
      z= modexp(7, (7293/2).floor, 342) = modexp(7, 3646, 342)
      modexp(7,3646, 342)
         3646 != 0
         z= modexp(7, 1823, 342)
         modexp(7, 1823, 342)

```
                    1823!=0
                    z=modexp(7, 911, 342)
                    modexp(7, 911, 342)
                          911 !=0
                          z=modexp(7, 455, 342)
                          modexp(7, 455, 342)
                                455 != 0
                                z=modexp(7, 227, 342)
                                modexp(7, 227, 342)
                                      227!=0
                                      z=modexp(7, 113, 342)
                                      modexp(7,113,342)
                                            113!=0
                                            z=modexp(7, 56, 342)
                                            modexp(7, 56, 342)
                                                  56!=0
                                                  z=modexp(7, 28, 342)
                                                  modexp(7, 56, 342)
                                                        28!=0
                                                        z=modexp(7, 14,
342)
                                                        modexp(7, 14,
342)
                                                              14!=0
                                                              z=modexp(7,
7, 342)
                                                              modexp(7,
7, 342)
                                                                    7!=0

      z=modexp(7, 3, 342)

      modexp(7, 3, 342)

      3.5!=0

      z=modexp(7, 1, 342)

      modexp(7, 1, 342)

      1!=0

      z=modexp(7, 0, 342)

      z=modexp(7, 0, 342)

      0=0 return 1

                  (7, 1, 342)  7*1^2mod 342=7
                  (7, 3, 342) 7*7^2mod 342 =1
                  (7, 7, 342) 7*1^2mod 342 =7
                  (7, 14, 342) 7^2mod 342 =49
                  (7, 28, 342) 49^2mod 342 =7
                  (7, 56, 342) 7^2mod 342 =49
                  (7, 113, 342) 7*49^2mod 342 = 49
                  (7, 227, 342) 7*49^2mod 342 = 49
                  (7, 455, 342) 7*49^2mod 342 = 49
                  (7, 911, 342) 7*49^2mod 342 = 49
                  (7, 1823, 342) 7*49mod 342 = 49
                  (7, 3646, 342) 49^2mod 342 = 7
```

(7,7293, 342) 7*7^2mod 342 = 1

4 my program takes n as the first command line arguement. I created the program so that it generates 2 prime numbers that can be represented by n bits,

when (n==8):
p = 137 q = 149
N= 20413
phi(N)= 20128
e = 63727
d= 10639
encry = 12010
decry = 2015
Time: a = 0.00006008148193 b = 0.00000500679016 c = 0.00000500679016

when (n==16):
p = 38371 q = 37529
N= 1440025259
phi(N)= 1439949360
e = 53558201
d= 319045961
encry = 786444927
decry = 2015
Time: a = 0.00011587142944 b = 0.00000500679016 c = 0.00000596046448

when (n==32p = 1756334123 q = 2588484973
N= 4546244484952633679
phi(N)= 4546244480607814584
e = 28752951799785419 51
d= 4419986731475234999
encry = 2179602887992434808
decry = 2015
Time: a = 0.00009703636169 b = 0.00002384185791 c = 0.00002384185791
):