Andrew Rutherford

CSCI 3104

CPU: 2.8 GHz Intel Core i7

Ram: 16 GB 1600 MHz DDR3

OSX Yosemite

Homework #2

On my honor, as a University of Colorado at Boulder student, I have neither given nor received

1 It takes O(mn) time to multiply x and y.

   a. Multiply(x, floor(y/2)) shifts y one bit a total of n number of times. The run time for this is O(n). Then either a multiplication by 2 or a multiplication by 2 and an addition will occur which is also O(n). These operations combined result in O(mn) running time.

2

   a. GCD:

      i. 770 = 2 * 5 * 7 * 11

      ii. 546 = 2 * 3 * 7 * 13

      iii. GCD = 2 * 7 = 14

   b. Euclid:

      i. Euclid(546, 770 mod 546) 770 mod 546 = 224

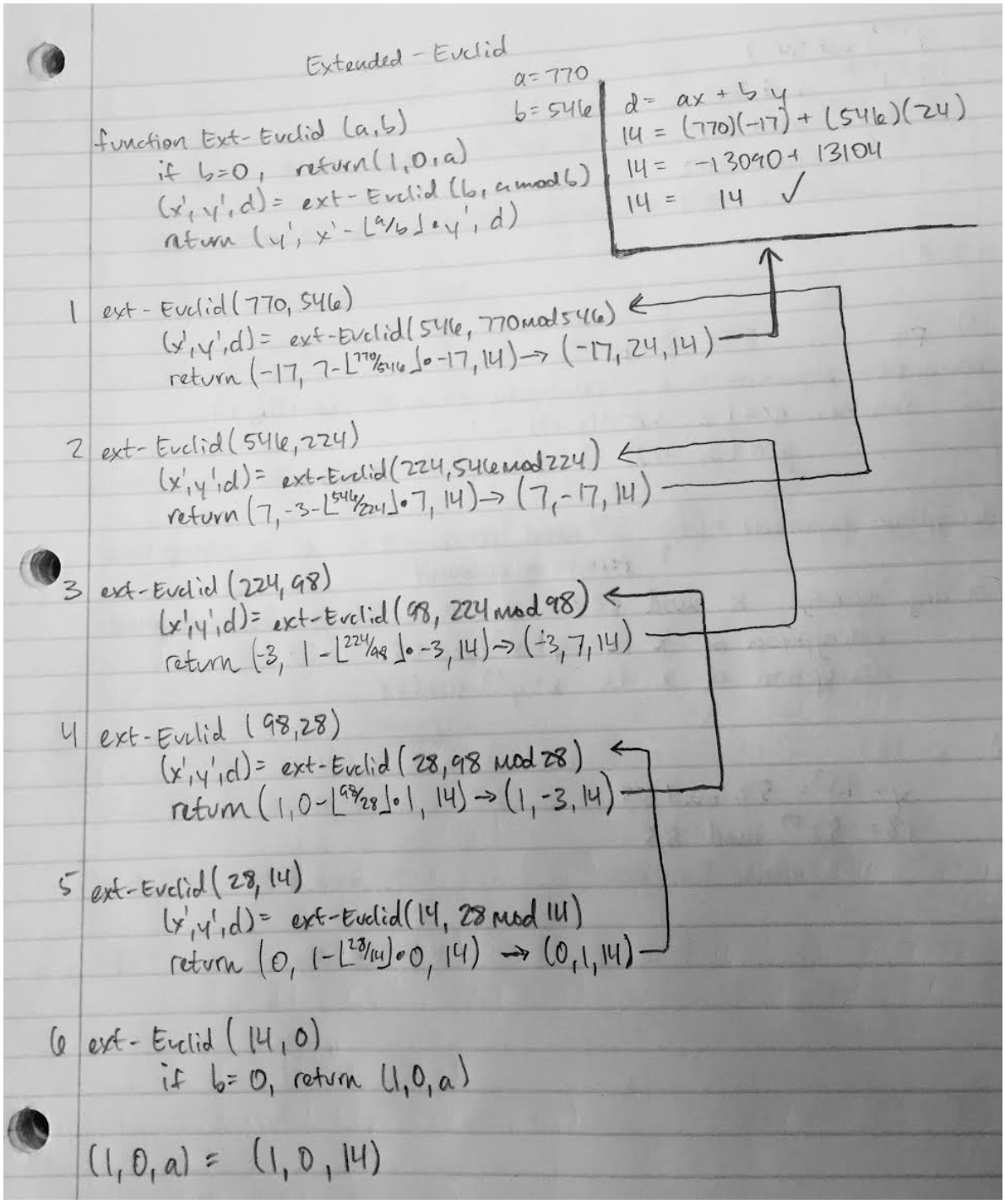
      ii. Euclid(224, 546 mod 224) 546 mod 224 = 98

      iii. Euclid(98, 224 mod 98) 224 mod 98 = 28

      iv. Euclid(28, 98 mod 28) 98 mod 28 = 14

v. Euclid(14, 28 mod 14) 28 mod 14 = 0

vi. If (b == 0) return a return 14



3

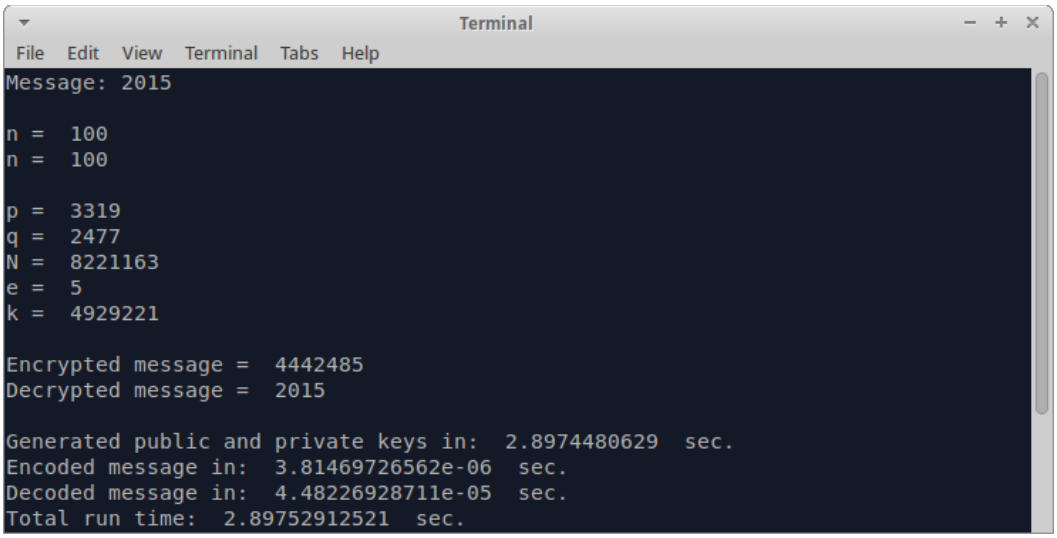
7^{7293} mod 342

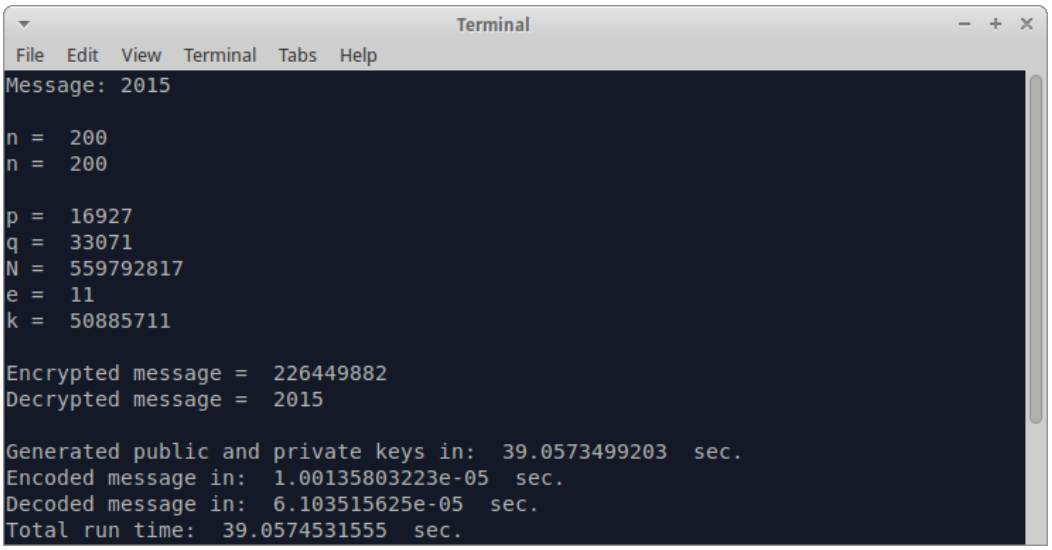
$(7^3)^{2431}$ mod 342

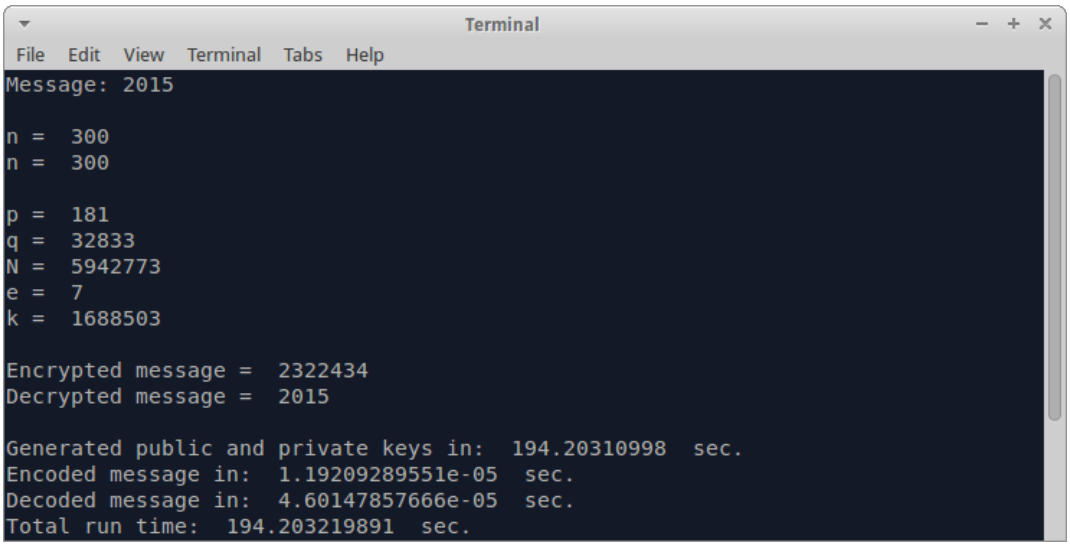
343^{2431} mod 342

1^{2431} mod 342

1 mod 342 = 1


Terminal
File Edit View Terminal Tabs Help
Message: 2015
n = 100
n = 100
p = 3319
q = 2477
N = 8221163
e = 5
k = 4929221
Encrypted message = 4442485
Decrypted message = 2015
Generated public and private keys in: 2.8974480629 sec.
Encoded message in: 3.81469726562e-06 sec.
Decoded message in: 4.48226928711e-05 sec.
Total run time: 2.89752912521 sec.


Terminal
File Edit View Terminal Tabs Help
Message: 2015
n = 200
n = 200
p = 16927
q = 33071
N = 559792817
e = 11
k = 50885711
Encrypted message = 226449882
Decrypted message = 2015
Generated public and private keys in: 39.0573499203 sec.
Encoded message in: 1.00135803223e-05 sec.
Decoded message in: 6.103515625e-05 sec.
Total run time: 39.0574531555 sec.


Terminal
File Edit View Terminal Tabs Help
Message: 2015
n = 300
n = 300
p = 181
q = 32833
N = 5942773
e = 7
k = 1688503
Encrypted message = 2322434
Decrypted message = 2015
Generated public and private keys in: 194.20310998 sec.
Encoded message in: 1.19209289551e-05 sec.
Decoded message in: 4.60147857666e-05 sec.
Total run time: 194.203219891 sec.