# Cryptography Homework 4--KEY

# Turn in

This data is the same for all three attempts:

p = 131

q = 157

n = 20567\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ p\*q

### Attempt 1, using Λ(n)

Λ(n) = 780\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ lcm(p-1, q-1)

e = 17\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(I chose 17, student choices will be different.)

gcd(e, Λ(n)) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ must equal 1. If not, pick a new e

d = 413\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ findModInverse(e, Λ(n))

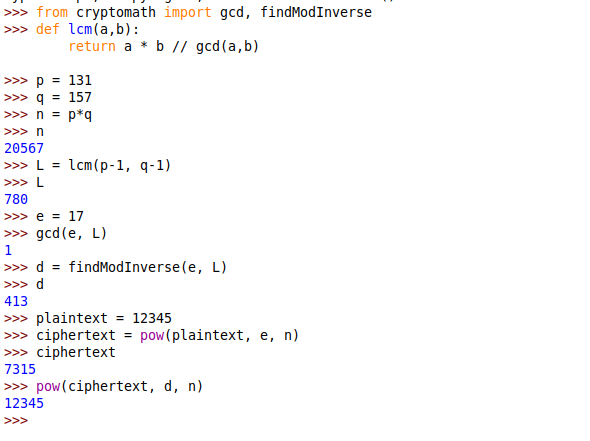
public key [n, e] [20567, 17]\_\_\_\_\_\_

private key [d, e] [20567, 413]\_\_\_\_\_

plaintext integer 12345\_\_\_\_\_\_\_\_\_

ciphertext 7315\_\_\_\_\_\_\_\_\_\_ pow(plaintext, e, n)

decrypted text 12345\_\_\_\_\_\_\_\_\_ pow(ciphertext, d, n)



### Attempt 2, using Φ(n)

Φ(n) = 20280\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (p-1)\*(q-1)

e = 17\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Use the same e that you used in Attempt 1

d = 1193\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ findModInverse(e, Φ(n))

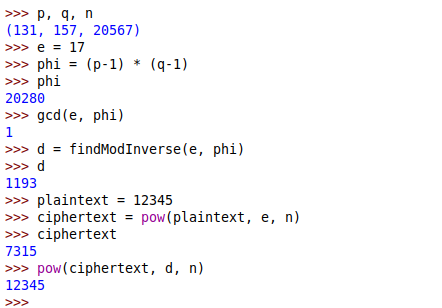
public key [n, e] [20567, 17]\_\_\_\_

private key [d, e] [20567, 1193]\_\_

plaintext integer 12345\_\_\_\_\_\_\_\_\_ Use the same plaintext that you used in Attempt 1

ciphertext 7315\_\_\_\_\_\_\_\_\_\_ pow(plaintext, e, n)

decrypted text 12345\_\_\_\_\_\_\_\_\_ pow(ciphertext, d, n)



### Attempt 3, using n (should fail)

n = 20567\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ n, same as above

e = 17\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Use the same e that you did in Attempt 1

d = 7259\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ findModInverse(e, n)

public key [n, e] [20567, 17]\_\_\_\_

private key [d, e] [20567, 7259]\_\_

plaintext integer 12345\_\_\_\_\_\_\_\_\_ Use the same plaintext that you used in Attempt 1

ciphertext 7315\_\_\_\_\_\_\_\_\_\_ pow(plaintext, e, n)

decrypted text 4726\_\_\_\_\_\_\_\_\_\_ pow(ciphertext, d, n)  
**Wrong!! You can compute d using either Λ(n) or Φ(n), but not using n !!!!!**

