Tristan Erney
November 23rd, 2021
Intro to Cryptology
Hands on Exercise 12

#1

p = 101
q = 113
phi(n) = (p – 1)(q – 1) = 100(112) = 11200

e * d = 1 (mod phi)
7467 * d = 1 (mod 11200)
d = 3

$m = C^d \pmod{n} = 5859^3 \pmod{11413} = 1415$

#2

P = 5
Q = 11
phi(n) = (p – 1)(q – 1) = 4(10) = 40

e * d = 1 (mod phi)
3 * d = 1 (mod 40)
d = 27

#3

$C = m^e \pmod{n}$

$C = 8^3 \pmod{437} = 75$
$C = 9^3 \pmod{437} = 292$

m = 8

#4

For e = 1, $C = m^e \pmod{n}$ would not change the plaintext since
the value of m would not change.
For e = 2, we need gcd(e, phi(n)) = 1 to find a private key.
If e = 2, then the gcd(e, phi(n)) = 2 which means a key does not exist.

#5

$A = 1^{13} \% 8881 = 1$
$B = 2^{13} \% 8881 = 8192$
$C = 3^{13} \% 8881 = 4624$
$D = 4^{13} \% 8881 = 4028$
$E = 5^{13} \% 8881 = 794$
$F = 6^{13} \% 8881 = 2343$
$G = 7^{13} \% 8881 = 231$
$H = 8^{13} \% 8881 = 4461$
$I = 9^{13} \% 8881 = 4809$

J = 10^{13} % 8881 = 3556
K = 11^{13} % 8881 = 476
L = 12^{13} % 8881 = 2015
M = 13^{13} % 8881 = 513
N = 14^{13} % 8881 = 699
O = 15^{13} % 8881 = 3603
P = 16^{13} % 8881 = 8078
Q = 17^{13} % 8881 = 2825
R = 18^{13} % 8881 = 8093
S = 19^{13} % 8881 = 2547
T = 20^{13} % 8881 = 1072
U = 21^{13} % 8881 = 2424
V = 22^{13} % 8881 = 633
W = 23^{13} % 8881 = 413
X = 24^{13} % 8881 = 5982
Y = 25^{13} % 8881 = 8766
Z = 26^{13} % 8881 = 1783

4461 = h
794 = e
2015 = l
2015 = l
3603 = o

p = hello