Anthony Constantino
HW6

Generate RSA key parameters where p=7 and q=13. 0 < e < 7.
Identify the RSA public key and the RSA private key.
Generate d using the extended Euclidean algorithm. Show detailed work. Do all work by hand.

Only e = 5 is co-prime so we will use e = 5

e = 5
p = 7
q = 13
n = p * q = 91
phi(n) = (p - 1) * (q - 1) = 72

GDC(72,5)
72 / 5 = 14 r 2 => 2 = 72(1) + 5(-14)
5 / 2 = 2 r 1 => 1 = 5(1) + 2(-2)
2 / 1 = 2 r 0 => 0 = 2(1) + 1(-2

72 / 5 = 14 r 2 => 2 = 72(1) + 5(-14)
5 / 2 = 2 r 1 => 1 = 5(1) + [72(1) + 5(-14)](-2)
= 5(1) + 72(-2) + 5(28)
= 5(29) + 72(-2)
2 / 1 = 2 r 0 => 0 = 2(1) + 1(-2)

5(29) + 72(-2) = GCD(72,5) = 1

d = 29