Scott Christensen

10/08/16

C.S. 465

H.W. # 7 Generate RSA Keys

P=7

Q=13

E=5 (Chosen arbitrarily from 0<e<7)

N=91 (P*Q)

Phi(N) = 72 ((P-1)*(Q-1))

For any given RSA implementation, the Public and Private Keys are both pairs.

Public Key = {E, N}

Private Key = {D, N}

To find D, we will use the extended Euclidean algorithm we learned about it class

Gcd(72, 5)

72%5 = 14 r 2

5%2 = 2 r 1

2%1 = 2 r 0

1%0 return 1

72 and 5 are relatively prime to one another.

Take the remainder formulas from above and substitute to find D:

2 = 72(1) + 5(-14)

1 = 5(1) + [72(1) + 5(-14)](-2)

1 = 5(1) + 72(-2) + 5(28)

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

D = 29