CS 465 HW 7 | RSA | Benjamin Bergeson

$p=7 \quad q=13 \quad 0<e<7 \quad e=5$

$n = p \cdot q = 91$

$\phi(n) = (p-1)\cdot(q-1) = (7-1)(13-1) = (6)(12) = 72$

Public Key = $(e,n) = (5, 91)$

360

$d = GCD(\phi(n), e) = GCD(72, 5)$

$GCD(72,5)$

$72/5 = 14 \text{ r } 2 \quad \Rightarrow 2 = 72(1) + 5(-14)$

$5/2 = 2 \text{ r } 1 \quad \Rightarrow 1 = 5(1) + 2(-2)$

$2/1 = 2 \text{ r } 0 \quad \Rightarrow 0 = 2(1) + 1(-2)$

$1/0$

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

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

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

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

$1 = 72(-2) + 5(29) \qquad d = 29 \quad k = -2$

Private Key = $(d,n) = (29, 91)$