Finding Public & Private Keys

$p = 13$, $q = 17$

$n = 221$

$\varphi(n) = (13-1)(17-1) = (12)(16) = 192$

$e \in (1, \ldots, 192)$

$\gcd(192, 5)$

$= \gcd(5, 2)$

$= \gcd(2, 1)$

$= \gcd(1, 0)$

$192/5 = 38$ remainder 2

$192 = 38(5) + 2$

$5/2 = 2$ remainder 1

$5 = 2(2) + 1$

$2/1 = 2$ remainder 0

$2 = 2(1) + 0$

$= 1$ ✓

$e = 5$ as $\gcd(5, 192) = 5$

$d = e^{-1} \bmod \varphi(n)$

java -jar JFLAP.1.jar &

(1)))

SPEED

gcd(192,5)=

gcd(5,2)

gcd(2,1)

192 = 187 + 5, 5 = 192 − 187

2 = 192 − 38(5)

1 = 5 − 4

= 5 − 2(2)

= 5 − 2(192 − 38(5))

= 5 − 2(192) + 76(5)

= −2(192) + 77(5)

d = 77

Encryption $y = x^e \bmod n$

$x = 71$, $e = 11$

$y = 71^{11} \bmod 77$

* Used online mod pow calc.

$y = 71$

Decryption

$x = y^d \bmod n$

$d = 77$, $n = 221$, $y = 220$

$x = 220^{77} \bmod 221$

* Used online mod pow calc.

$x = 220$