RSA: (Rivest Shamir Adleman)

I Select 2 large Prime Numbers
p & q → p = 13 q = 11

II Compute n
n = p * q → n = 13 * 11 = 143

III Compute $\phi(n)$ ← Euler's totient fn
$\phi(n) = \phi(p) * \phi(q)$
∵ p & q are prime
∴ $\phi(p) = p - 1$
$\phi(q) = q - 1$
→ $\phi(n) = \phi(p) * \phi(q)$
$= 12 * 10 = 120$

IV Now select the public key e,
① $0 < e < \phi(n)$
② $GCD(e, \phi(n)) = 1$
→ e = 13

V Now calculate private key d,
$d \equiv e \bmod \phi(n)$
⇒ $de^{-1} \bmod \phi(n) = 1$

$$\begin{cases} d \equiv e \bmod \phi(n) \\ de^{-1} \bmod \phi(n) = 1 \\ d\,13^{-1} \bmod 120 = 1 \end{cases}$$

1, 2, 3, 4 ...

$d = \frac{\phi(n)^0 + 1}{e}$

$d = \frac{120 * 1 + 1}{13} = 9.3$

$d = \frac{120 * 2 + 1}{13} = 18.5$

$d = \frac{120 * 3 + 1}{13} = 27.8$

$d = \frac{120 * 4 + 1}{13} = 37$

* Continue till answer is Integer.

VI Public key (e, n)
Private key (d, n)
Public (13, 143)
Private (37, 143)

VII To Encrypt:
$C = P^e \bmod n$

VIII To decrypt:
$P = C^d \bmod n$

C: Cipher text P: Plain text

E (13, 143)

$C = P^e \bmod n$

Note: $P < n$

eg $P = 5$

$C = 5^{13} \bmod 143$

$C_1 = 5^1 \bmod 143 = 5$

$C_2 = 5^4 \bmod 143 = 9$ ~~53~~

$C_3 = 5^8 \bmod 143 = 92$

$C = [(C_1 * C_2 * C_3) \bmod 143]$

$C = 70$

D (37, 143)

$P = C^d \bmod n$

$C = 70$

$P = 70^{37} \bmod 143$

$P_1 = (70^{16} \bmod 143) = 92$

$P_2 = (70^{16} \bmod 143) = 92$

$P_3 = (70^4 \bmod 143) = 14$

$P_4 = (70 \bmod 143) = 70$

$P = [(P_1 \times P_2 \times P_3 P_4) \bmod 143]$

$P = 5$