RSA KEY GENERATION ALGORITHM

AGNI DATTA

0.1 Select two huge primes numbers,

p and q

0.2 Calculate,

$n = p \times q$

0.3 Calculate Euler's Totient[1] Function,

$\varphi(n) = (p - 1) \times (q - 1)$

0.4 Choose the value of e such that,

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

0.5 Public Key Pair,

$\{e, n\}$

0.6 Private Key Pair,

$\{d, n\}$

[1] refer https://en.wikipedia.org/wiki/Euler%27s_totient_function