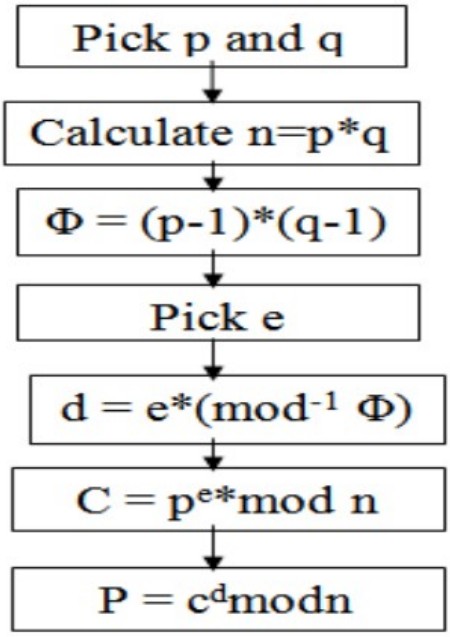
Lab Assignment No. 8

Write a C/C++/Python/JAVA program to implement RSA algorithm. Use following algorithmic steps to implement.

Flowchart:



Algorithm:

STEP-1: Select two co-prime numbers as p and q.

STEP-2: Compute n as the product of p and q.

STEP-3: Compute (p-1)*(q-1) and store it in z.

STEP-4: Select a random prime number e that is less than that of z.

STEP-5: Compute the private key, d as e * $mod^{-1}(z)$.

STEP-6: The cipher text is computed as $message^{e}$ * mod n.

STEP-7: Decryption is done as $cipher^{d}$mod n.