RSA ALGORITHM

CODE:

```
import math
p = int(input("enter p : "))
q = int(input("enter q : "))
message = int(input("enter message : "))
d=0
# calculate n
n = p*q
# claculate totient
totient = (p-1)*(q-1)



for e in range(2, totient):
   if math.gcd(e, totient) == 1:
      break

for i in range(1, 10):
   x = 1 + i*totient
   if x % e == 0:
      d = int(x/e)
      break

local_cipher =pow(message, e)
cipher_text = local_cipher % n

decrypt_t= pow(cipher_text, d)
decrpyted_text = decrypt_t % n
```

```
print('n = '+str(n))

print('e = '+str(e))

print('totient = '+str(totient))

print('d = '+str(d))

print('cipher text = '+str(cipher_text))

print('decrypted text = '+str(decrpyted_text))
```

OUTPUT: