**Q: Create one public key and one private key of RSA**

**PROGRAM**

clc;

clear all;

close all;

pkg load communications

disp('Creating pair of RSA keys');

p=input('Input prime number p = ');

q=input('Input prime number q = ');

n = p \* q;

fprintf('\nn = %d',n);

%Calculating phi

phi=(p-1)\*(q-1);

tmpValue=0;

gcdValue=0;

fprintf('\nphi(%d) = %d',n,phi);

%Choose a random number 𝑒

while(gcdValue~=1||tmpValue==0)

e1=randint(1,1,n);

e=randint(1,1,e1);

tmpValue=isprime(e);

gcdValue=gcd(e,phi);

end

fprintf('\ne = %d',e);

%Calculating modulus "d" using Extended Euclidean algorithm

tmpValue1=0;

d=0;

while(tmpValue1~=1);

d=d+1;

tmpValue1=mod(d\*e,phi);

end

fprintf('\nd = %d',d);

%Printing pair of keys

fprintf('\nObtained Public key = (%d,%d)',n,e);

fprintf('\nObtained Private key = (%d,%d)\n\n',n,d);

**OUTPUT**

