



Ministry of Higher Education And Scientific Research

AL-Mustaqbal University College

Department of Computer Engineering Techniques

Experiment 10

RSA decryption

Eng:- Shaymaa Fakhir AL-Hamdany

Decrypt RSA Cipher:

```
clc; clear all; close all
p=input('enter first prime number p: ');
q=input('enter second prime number q: ');
n=p*q;
phi=(p-1)*(q-1);
e=input('enter the key e: ');
if gcd(phi,e)~=1
    disp(['this value of d is incorrect, e is not found'])
else
    for i=1:phi
        if mod(e*i,phi)==1
            d=i
        end
    end
end
c=input('enter ciphertext in number: ');
c1=0;
f=1;
b= fliplr(dec2bin(d));
k=length(b);
for i=k:-1:1
    c1=c1*2;
    f=mod(f*f,n);
    if b(i)=='1'
        c1=c1+1;
        f=mod(f*c,n);
    end
end
end
m=f;
```