Lab Report 8

ESE – 3014

EMBEDDED SYSTEMS COMMUNICATION PROTOCOLS AND SECURITY

Submitted to :

Linchan Wang

Submitted by:

Gurvinder Singh(748418)

**1. Simulate encryption communication, encrypt a message use a RSA publickey, and try to decrypt it with a RSA private key.**

Solution:-

l = 77

m = 17

t = l \* m;

phi = (l – 1) \* ( m-1)

f = 23;

c = 0;

d = 0;

while (c ~ = 1)

d = d+1;

c = mod ( d\*f, phi);

end

function krep = Denc (a,b,c)

if (b==0)

Denc = 1 ;

elseif (mod (b,2) ==0)

d = Denc (a,b/2,c);

Denc = mod( d\*d,c );

else

s=frep(a,b-1,c);

Denc=mod((mod(a,b)\*s),c);

endif

endfunction

fprintf("\n public key (%d,%d)",t,f);

fprintf("\n private key (%d,%d )",t,d);

message1 = 43

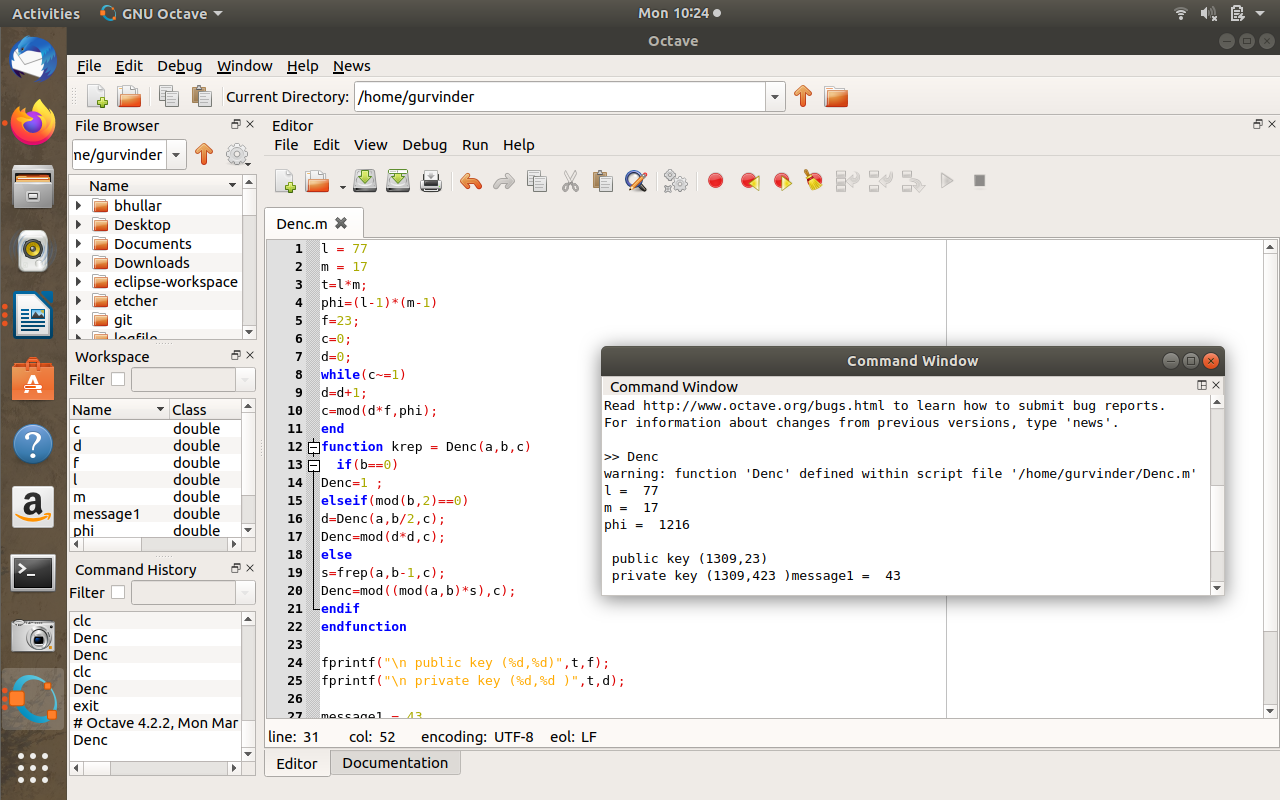
c = Denc(message1,f,t);

fprintf ("\n encrypted message: %d ",c);

message2 = Denc(c,d,t);

fprintf ("\n original message: %d", message2);output

**Output:**



**2. Try to crack a private key with a known public key. And determine thekey component to keep the security of RSA encryption communication.Hint: the key is find outd, we can get private key once we haved. Is itpossible to derivedin the case ofnande?**

**1. ed≡(modφ(n))**

**2.φ(n) = (p-1)(q-1)**

**3. n=pq**

Solution:

n=2431

e=17

fac=factor(n)

phi=((fac(1,1)-1)\*(fac(1,2)-1))

z=0;

j=0;

while(z~=1)

j=j+1;

z=mod(j\*e,phi);

end

fprintf("\n value of d is %d",j);

**Output:**

