**Diffie – Hellman Key Exchange**

clc;

close all;

clear all;

p=input('Enter value of p: ');

a=input('Enter value of a: ');

Xa=input('Enter value of Xa: ');

Xb=input('Enter value of Xb: ');

[ans, b, product]=sqmod(a,Xa,p);

Ya=ans

[ans, b, product]=sqmod(a,Xb,p);

Yb=ans

[ans, b, product]=sqmod(Yb,Xa,p);

k1=ans;

[ans, b, product]=sqmod(Ya,Xb,p);

k2=ans;

if(k1==k2)

disp('Exchange Key')

k=k1;

k

end

function [ ans, b, product] = sqmod( a,x,n )

%UNTITLED2 Summary of this function goes here

% Detailed explanation goes here

n1=dec2bin(x);

product=1;

l1=length(n1);

b=zeros(1,l1);

temp=a;

b(1)=mod(temp,n);

for i=2:l1

temp=b(i-1)\*b(i-1);

b(i)=mod(temp,n);

end

for i=1:l1

if(n1(i)=='1')

product=product\*b(l1-i+1);

end

end

ans = mod(product,n);

end

Output:

Enter value of p: 19

Enter value of a: 3

Enter value of Xa: 93

Enter value of Xb: 273

Ya = 8

Yb = 8

Exchange Key

k = 18