#----------------------------------------------------------------------------------

#Rutvik Parmar

#H-41

#Date – 21st April 2016

#Assignement No:9 – Diffie Hellman Key exchange

#----------------------------------------------------------------------------------

**import** java.io.\*;  
**import** java.math.BigInteger;  
**class** Diffie  
{  
 **public static void** main(String[]args)**throws** IOException  
 {  
 BufferedReader br=**new** BufferedReader(**new** InputStreamReader(System.***in***));  
 System.***out***.println(**"Enter prime number:"**);  
 BigInteger p=**new** BigInteger(br.readLine());  
 System.***out***.print(**"Enter primitive root of "**+p+**":"**);  
 BigInteger g=**new** BigInteger(br.readLine());  
 System.***out***.println(**"Enter value for x less than "**+p+**":"**);  
 BigInteger x=**new** BigInteger(br.readLine());  
 BigInteger R1=g.modPow(x,p);  
 System.***out***.println(**"R1="**+R1);  
 System.***out***.print(**"Enter value for y less than "**+p+**":"**);  
 BigInteger y=**new** BigInteger(br.readLine());  
 BigInteger R2=g.modPow(y,p);  
 System.***out***.println(**"R2="**+R2);  
 BigInteger k1=R2.modPow(x,p);  
 System.***out***.println(**"Key calculated at Alice's side:"**+k1);  
 BigInteger k2=R1.modPow(y,p);  
 System.***out***.println(**"Key calculated at Bob's side:"**+k2);  
 System.***out***.println(**"deffie hellman secret key Encryption has Taken"**);  
 }  
}

Output -

Enter prime number:

11

Enter primitive root of 11: 7

Enter value for x less than 11:

3

R1=2

Enter value for y less than 11: 6

R2=4

Key calculated at Alice's side:9

Key calculated at Bob's side:9

deffie hellman secret key Encryption has Taken

**­­­C code**

#include<stdio.h>

int main()

{

int p,g;

printf("\n\nEnter the publicly shared prime - ");

scanf("%d",&p);

printf("\nEnter the primitive root modulo of prime - ");

scanf("%d",&g);

int a,b;

printf("\nEnter the secret keys for Alice and Bob - ");

scanf("%d%d",&a,&b);

int A = 1,B = 1;

for(int i = 0; i<a; i++)

{

A = (A\*g)%p;

}

A = A%p;

printf("\nAlice sends over a public channel - %d", A);

for(int i = 0; i<b; i++)

{

B = (B\*g)%p;

}

B = B%p;

printf("\nBob sends over a public channel - %d", B);

printf("\n\nPrivately Calculated Shared Secret\n\n");

int s1 = 1,s2 = 1;

for(int i = 0; i<a; i++)

{

s1 = (s1\*B)%p;

}

s1 = s1%p;

printf("\n\tAlice Shared Secret - %d",s1);

for(int i = 0; i<b; i++)

{

s2 = (s2\*A)%p;

}

s2 = s2%p;

printf("\n\tBob's Shared Secret - %d\n\n",s2);

}

**Python Code**

|  |
| --- |
| # use Python 3 print function  # this allows this code to run on python 2.x and 3.x  from \_\_future\_\_ import print\_function    # Variables Used  sharedPrime = 23    # p  sharedBase = 5      # g    aliceSecret = 6     # a  bobSecret = 15      # b    # Begin  print( &amp;amp;amp;amp;amp;amp;quot;Publicly Shared Variables:&amp;amp;amp;amp;amp;amp;quot;)  print( &amp;amp;amp;amp;amp;amp;quot;   Publicly Shared Prime: &amp;amp;amp;amp;amp;amp;quot; , sharedPrime )  print( &amp;amp;amp;amp;amp;amp;quot;   Publicly Shared Base:  &amp;amp;amp;amp;amp;amp;quot;, sharedBase )    # Alice Sends Bob A = g^a mod p  A = (sharedBase\*\*aliceSecret) % sharedPrime  print( &amp;amp;amp;amp;amp;amp;quot;\n Alice Sends Over Public Chanel: &amp;amp;amp;amp;amp;amp;quot; , A )    # Bob Sends Alice B = g^b mod p  B = (sharedBase \*\* bobSecret) % sharedPrime  print( &amp;amp;amp;amp;amp;amp;quot;   Bob Sends Over Public Chanel: &amp;amp;amp;amp;amp;amp;quot;, B )    print( &amp;amp;amp;amp;amp;amp;quot;\n------------\n&amp;amp;amp;amp;amp;amp;quot; )  print( &amp;amp;amp;amp;amp;amp;quot;Privately Calculated Shared Secret:&amp;amp;amp;amp;amp;amp;quot; )  # Alice Computes Shared Secret: s = B^a mod p  aliceSharedSecret = (B \*\* aliceSecret) % sharedPrime  print( &amp;amp;amp;amp;amp;amp;quot;   Alice Shared Secret: &amp;amp;amp;amp;amp;amp;quot;, aliceSharedSecret )    # Bob Computes Shared Secret: s = A^b mod p  bobSharedSecret = (A\*\*bobSecret) % sharedPrime  print( &amp;amp;amp;amp;amp;amp;quot;   Bob Shared Secret: &amp;amp;amp;amp;amp;amp;quot;, bobSharedSecret ) |