PROGRAM:

```
package dsa;
import java.util.*;
import java.math.BigDecimal;
import java.math.BigInteger;
public class DSA
{
public static void main(String[] args) {
Scanner sc=new Scanner(System.in);
int l,p,q,n,h,X,m,k,temp,temp1,i,kinv=0,w=0;
boolean f=false;
BigInteger K1,K2,g,Y,rt,r,Ki,M,x,stemp,s,W,U1,U2,Vtemp,v;
double j=0;
System.out.println("***** WELCOME TO DSS ALGORITHM *****");
System.out.println();
System.out.println("Enter the value of l:");
l=sc.nextInt();
System.out.println("Enter the value of p such that it is prime:");
p=sc.nextInt();
if((p<Math.pow(2,l))&&(p>=Math.pow(2,l-1))){
for(i=2;i<=p/2;++i){
if(p%i==0){
f=true;
break;
}
}
if(!f){
System.out.println("Enter the value of n:");
n=sc.nextInt();
```

```
System.out.println("Enter the value of q such that it is a prime divisor of p-1:");
q=sc.nextInt();
if((q<Math.pow(2,n))&&(q>=Math.pow(2,n-1))){
for(i=2;i<=q/2;++i){
if(q%i==0){
f=true;
break;
}
}
if(!f){
if((p-1)%q==0){
System.out.println("Enter the value of h:");
h=sc.nextInt();
K1=BigInteger.valueOf(p);
K2=BigInteger.valueOf(q);
System.out.println("\nCOMPUTING THE VALUE OF g...\n");
temp=(p-1)/q;
BigInteger H=BigInteger.valueOf(h);
g=(H.pow(temp)).mod(K1);
System.out.println("The value of g is: "+g);
System.out.println("\nGETTING USER'S PRIVATE KEY X...\n");
System.out.println("Enter the value of user's private key X:");
X=sc.nextInt();
Y=(g.pow(X)).mod(K1);
System.out.println("The value of Y is: "+Y);
System.out.println("\nSIGNING IS PERFORMED...\n");
System.out.println("Enter the value of m:");
m=sc.nextInt();
System.out.println("Enter the value of k:");
k=sc.nextInt();
```

```
rt=(g.pow(k)).mod(K1);
r=rt.mod(K2);
for(i=0;i<Integer.MAX_VALUE;i++){
if((k*i)%q==1){
kinv=i;
break;
}
}
Ki=BigInteger.valueOf(kinv);
x=BigInteger.valueOf(X);
M=BigInteger.valueOf(m);
stemp=(M.add((x.multiply(r))));
s=(Ki.multiply(stemp)).mod(K2);
System.out.println("Sign = ( "+r+","+s+" )");
System.out.println("\nVERIFICATION OF PROCESS...\n");
for(i=0;i<Integer.MAX_VALUE;i++){
if(((s.intValueExact())*i)%q==1){
w=i;
break;
}
}
W=BigInteger.valueOf(w);
System.out.println("The value of w is: "+W);
U1=(M.multiply(W)).mod(K2);
U2=(r.multiply(W)).mod(K2);
System.out.println("The value of U1 is: "+U1);
System.out.println("The value of U2 is: "+U2);

Vtemp=((g.pow(U1.intValueExact())).multiply((Y.pow(U2.intValueExact())))).mod(K1);
v=Vtemp.mod(K2);
```

```
System.out.println("The value of v is: "+v);

if(v.equals(r)){
System.out.println("No tampering has occurred..Our data is safe!");
}
else{
System.out.println("Tampering has occurred in our data!");
}
}
else{
System.out.println("Not a divisor!");
}
}
else{
System.out.println("Not a prime!");
}
}
else{
System.out.println("Value of q is not in range!");
}
}
else{
System.out.println("Not a prime!");
}
}
else{
System.out.println("Value of p is not in range!");
}
}
}
```

MEENAKSHI SUNDARARAJAN ENGINEERING COLLEGE

#363,Arcot Road, Kodambakkam, Chennai – 600024, Tamil Nadu, India

Department: Computer Science & Engineering **Register No:311519104006**

OUTPUT:

```
<terminated> DSA [Java Application] C:\Users\Akshwarya\.p2\pool\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64_17.0.5.v20221102-0933\jre\bin\javaw.exe  (04
***** WELCOME TO DSS ALGORITHM *****

Enter the value of l:
13
Enter the value of p such that it is prime:
7879
Enter the value of n:
7
Enter the value of q such that it is a prime divisor of p-1:
101
Enter the value of h:
5

COMPUTING THE VALUE OF g...

The value of g is: 590

GETTING USER'S PRIVATE KEY X...

Enter the value of user's private key X:
75
The value of Y is: 687

SIGNING IS PERFORMED...

Enter the value of m:
22
Enter the value of k:
50
Sign = ( 72,64 )

VERIFICATION OF PROCESS...

The value of w is: 30
The value of U1 is: 54
The value of U2 is: 39
The value of v is: 72
No tampering has occurred..Our data is safe!
```