EXPNO:6 **DATE:**

DSA

Aim: ToimplementDigitalSignatureAlgorithm(DSA)usingC.

Algorithm:

- Step1:Includethenecessaryheaderfiles#include<stdio.h>and#include <math.h>.
- Step2:Declaretherequiredvariablesfortheprogram,includingintegersfor primenumbers,privatekeys,hashvalue,andcomputedvalueslikeg,r, and s.
- Step3:Prompttheusertoentertheprimenumberpandtheprimedivisor qof(−1)(p−1).Also,prompttheusertoenter*h*hsuchthatit'sgreaterthan 1 and less than (−1)(p−1).
- Step4:Calculategusingthefunctionpower(h,t,p).
- Step5:Prompttheusertoentertheirprivatekeyxandper-messagesecret keyk.Also,prompttheusertoenterthehashvalueM.
- Step6:Computerandsvaluesforthesignatureusingtheprovided formulas.
- Step7:Printthecomputedvaluesofg,y,r,ands.
- Step8:Definethepowerfunctiontocalculatethepowerofa numbermodulo p.
- Step9:DefinethemultiplicativeInversefunctiontofindthemultiplicative inverse of a number modulo n.

Program:

```
#include<stdio.h>
#include<math.h>
 int power(int,unsigned int,int);
intmultiplicativeInverse(int,int,int);
int main() {
intp,q,h,g,r,s,t,x,y,z,k,inv,hash;
```

```
printf("\nEnterprimenumberpandenterqprimedivisorof(p-1):"); scanf("%d
%d",&p,&q);
printf("\nEnterhsuchthatitgreaterthan1andlessthan(p-1):"); scanf("%d",&h); g
= power(h,t,p);
printf("\nEnteruser'sprivatekeysuchthatitisgreaterthan0andlessthanq:");
scanf("%d",&x);
printf("\nEnteruser'sper-messagesecretkeyksuchthatitisgreaterthan0andless than q :
");
scanf("%d",&k);
printf("\nEnterthehash(M)value:");
scanf("%d",&hash);
r=z%q;inv=multiplicativeInverse(k,q,p);
s = inv * (hash + x * r) % q;
printf("\n*********Computed Values*********");
printf("\ng = %d",g); printf("\ny = %d",y);
printf("\nGeneratedSignatureSender=(%d,%d)\n",r,s);
}
intpower(intx,unsignedinty,intp)
{intres=
1;x =
x% p;
{
res=(res*x)%p;
}return
res; }
intmultiplicativeInverse(inta,intb,intn)
{
intsum,x,y;for(y=0;y<n;y++)
{
for(x=0;x<n;x++)
{
sum=a*x+b*(-y); if(sum
== 1) return
x;
}
```

```
}
}
```

Output:

```
/tmp/RlSBPZ6YGG.o

Enter prime number p and enter q prime divisor of (p-1): 9
9

Enter h such that it greater than 1 and less than (p-1): 6

Enter user's private key such that it is greater than 0 and less than q : 4

Enter user's per-message secret key k such that it is greater than 0 and less than q :
    3

Enter the hash(M) value : 1

*********Computed Values*********
g = 6
y = 0
Generated Signature Sender = (6, 0)


=== Code Execution Successful ===
```

Result: