Practical no: 7

Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Cryptography Lab

Aim: Implementation of Digital Signature Standard

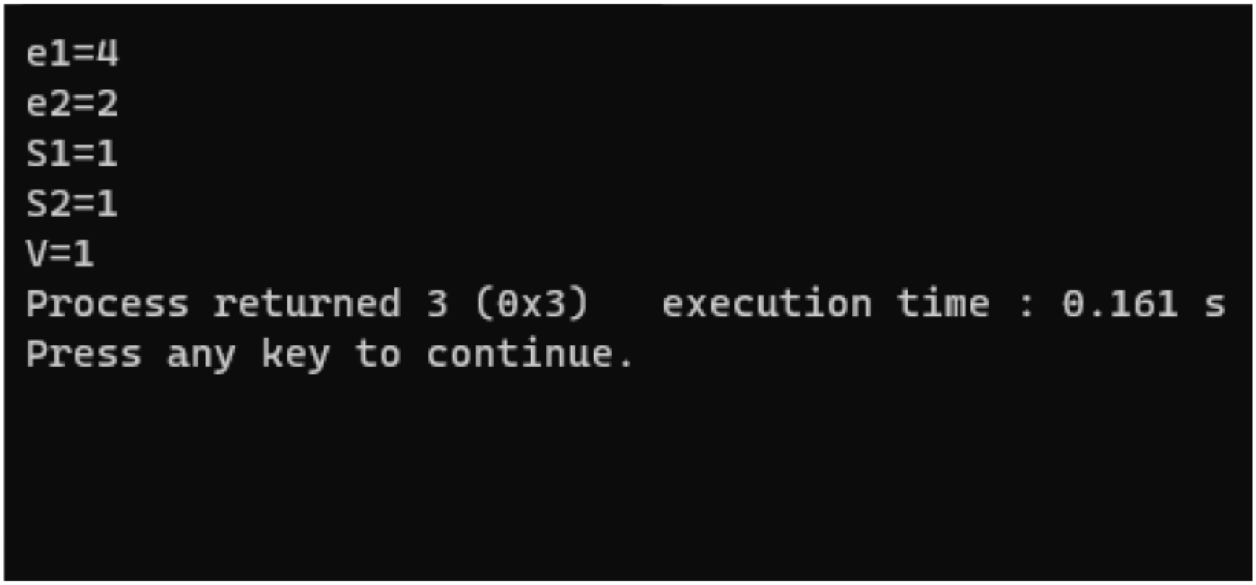
Code and Output:

1. With same h(M) value passing in the calculation of S1 and V:

```
#include<stdio.h>
#include<conio.h>
#include<math.h>
int power(long int a, long int j, long int c)
{
   int f,i;
   f=1;
   for(i=1;i<=j;i++)
   {
      f=(f*a)%c;
   }
   f=f%c;
   return f;
}

void main()
{
   int S1,M,D,S2,r,p,q,e0,e1,a,d,e2,V,T,F,k,l,z;
   d=11;
   M=9;
   p = 7;
   q = 3;
   e0 = 5;
   a = (p-1)/q;
   r=3;
   e1 = power(e0,a,p);
   e2=power(e1,d,p);
   printf("e1=%d\n",e1);
   printf("e2=%d\n",e2);
```

```
    S1= power(e1,r,p);
    S1= power(S1,1,q);
    printf("S1=%d\n",S1);
    D=(M + d*S1)/r;
    S2=power(D,1,q);
    printf("S2=%d\n",S2);
    T=M *(1/S2);
    F=S1*(1/S2);
    k=power(e1,T,p);
    l=power(e2,F,p);
    z=k*l;
    V=power(z,1,p);
    V=power(V,1,q);
    printf("V=%d\n",V);
}
```

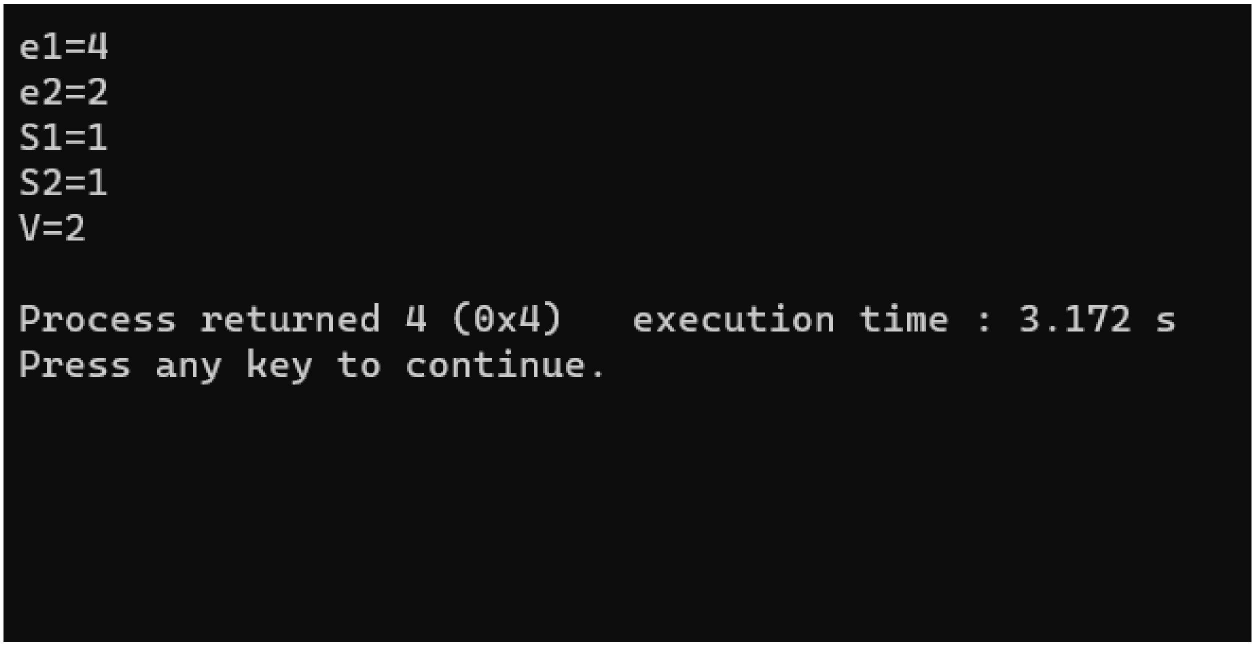


```
e1=4
e2=2
S1=1
S2=1
V=1
Process returned 3 (0x3)   execution time : 0.161 s
Press any key to continue.
```

2. With different h(M) values passing in the calculation of S1 and V:

```
#include<stdio.h>
#include<conio.h>
#include<math.h>
int power(long int a, long int j, long int c)
{
    int f,i;
    f=1;
    for(i=1;i<=j;i++)
    {
        f=(f*a)%c;
    }
    f=f%c;
    return f;
}

void main()
{
    int S1,M,D,S2,r,p,q,e0,e1,a,d,e2,V,T,F,k,l,z;
    d=11;
    M=10;
    p = 7;
    q = 3;
    e0 = 5;
    a = (p-1)/q;
    r=3;
    e1 = power(e0,a,p);
    e2=power(e1,d,p);
    printf("e1=%d\n",e1);
    printf("e2=%d\n",e2);
    S1= power(e1,r,p);
    S1= power(S1,1,q);
    printf("S1=%d\n",S1);
    D=(M + d*S1)/r;
    S2=power(D,1,q);
    printf("S2=%d\n",S2);
    T=9 *(1/S2);
    F=S1*(1/S2);
    k=power(e1,T,p);
    l=power(e2,F,p);
    z=k*l;
    V=power(z,1,p);
    V=power(V,1,q);
    printf("V=%d\n",V);
}
```



```
e1=4
e2=2
S1=1
S2=1
V=2

Process returned 4 (0x4)   execution time : 3.172 s
Press any key to continue.
```