Practical no: 5

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

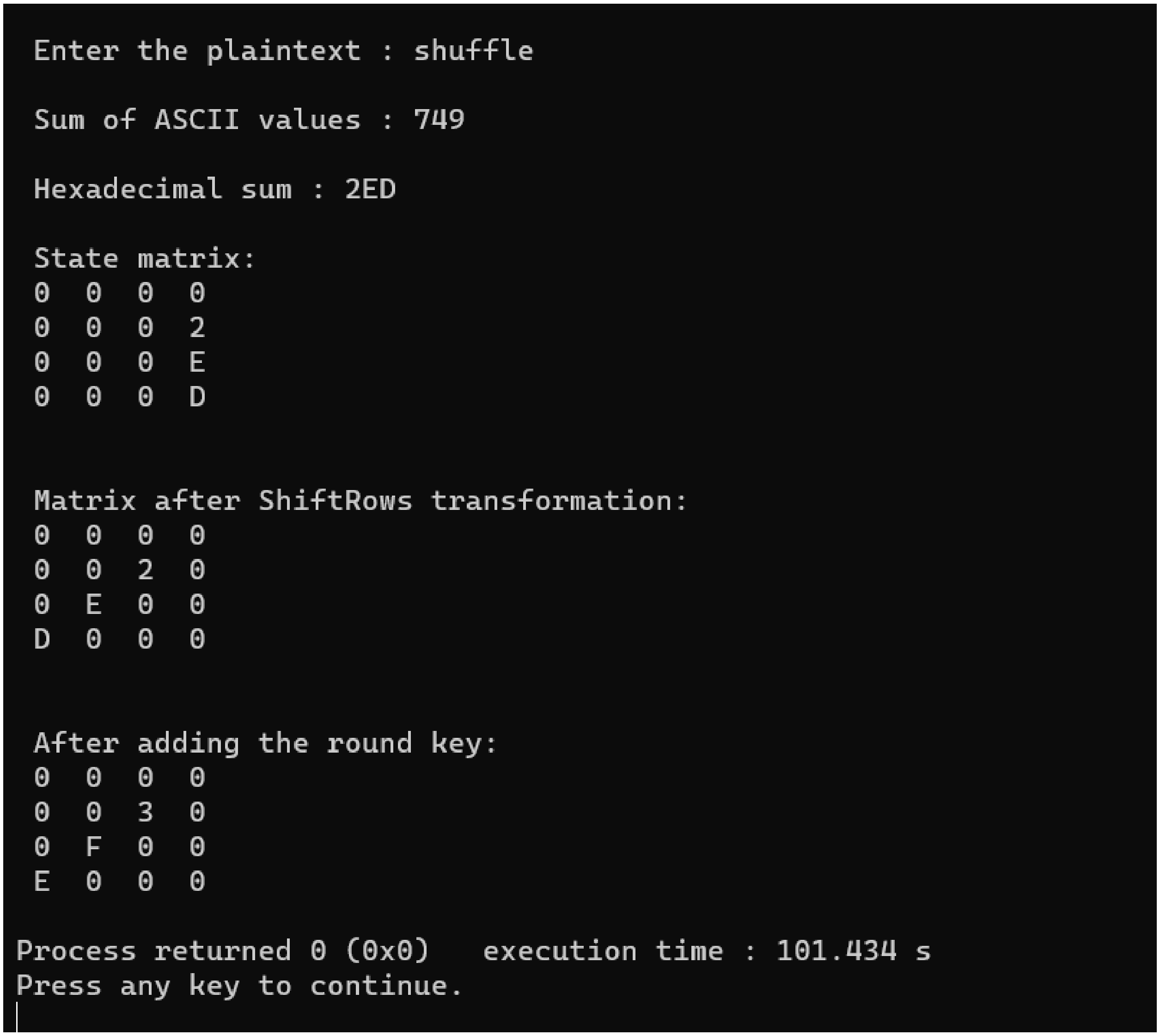
Aim: Implementation of AES

Code and Output:

```
#include<stdio.h>
#include<string.h>
#include<math.h>
int main(){
char str[16];
int i = 0, j, temp,k,d,x;
char hexa[16];
char mat[4][4];
int mat3[4][4];
int mat4[4][4]={{0,0,0,0},{0,0,1,0},{0,1,0,0},{1,0,0,0}};
int sum=0;
printf("\n Enter the plaintext : ");
scanf("%s",str);
int flag=1;
for(j=0;j<16;j++)
{
   if(flag==1)sum+=str[j];
   if(str[j]=='\0')
   {
     flag=0;
     str[j]=(char)0;
   }
}
printf("\n Sum of ASCII values : %d \n",sum);
d=sum;
while (d > 0)
{
    temp = d % 16; if (temp < 10)
    temp = temp + 48;
    else
    temp = temp + 55;
    hexa[i++] = temp; d = d / 16;
}
hexa[i]='\0';
printf("\n Hexadecimal sum : %s \n",strrev(hexa));
k=15;
int l=i;
for(x=0;x<4;x++)
   {
    for(j=0;j<4;j++)
       {
          if
            (k>i-1)mat[j][x]='0';
          else
             mat[j][x]=(char)hexa[l-i--];
    k--;
}
}
printf("\n State matrix:\n");
for(i=0;i<4;i++)
{
    for(j=0;j<4;j++)
   {
       printf(" %c ",mat[i][j]);
   }
   printf("\n");
}
printf("\n"); //shift
int shift=0;
char mat2[i][j];
for(i=0;i<4;i++)
{
   shift=i;
   for(j=0;j<4;j++)
   {
      if(shift+j<=3)
      mat2[i][j]=mat[i][j+shift];
      else
      mat2[i][j]=mat[i][j-1];
   }
}
printf("\n Matrix after ShiftRows transformation:\n");
for(i=0;i<4;i++)
{
   for(j=0;j<4;j++)
   {
      printf(" %c ",mat2[i][j]);
   }
   printf("\n");
}
   char hexDigits[16] = { '0', '1', '2', '3', '4', '5', '6', '7',
                          '8', '9', 'A', 'B', 'C', 'D', 'E', 'F' };
   char hexadecimalnumber;
   int  power = 0, digit=0,decimalnumber=0;
   printf(" \n ");

printf("\n After adding the round key:\n");
for(i=0;i<4;i++)
{
   for(j=0;j<4;j++)
   {
      hexadecimalnumber = mat2[i][j];
      for (k = 0; k < 16; k++)
      {
         if (hexadecimalnumber == hexDigits[k])
         {
            decimalnumber = k;
         }
      }
      mat3[i][j] = decimalnumber;
   printf(" %C ",hexDigits[mat3[i][j]+mat4[i][j]]);
```

```
    }
    printf("\n");
}
return 0;
}
```



```
 Enter the plaintext : shuffle

 Sum of ASCII values : 749

 Hexadecimal sum : 2ED

 State matrix:
 0  0  0  0
 0  0  0  2
 0  0  0  E
 0  0  0  D


 Matrix after ShiftRows transformation:
 0  0  0  0
 0  0  2  0
 0  E  0  0
 D  0  0  0


 After adding the round key:
 0  0  0  0
 0  0  3  0
 0  F  0  0
 E  0  0  0

Process returned 0 (0x0)   execution time : 101.434 s
Press any key to continue.
```