Name: Santhosh J

Register number: 312217104142

IT8761-Security Lab SEMESTER PRACTICALS

|       | Names. Santhorh - J  |
|-------|--|
|       | 10017104142  |
|       | 1 1/2 2/2  |
|       | IT876  |
| 1000  | Rubject Coder Security Lab. I Envinering.  |
| 2011  | and Engineering  |
|       | Subject code IT& 76 Lab. Subject rame Security Lab.  Branch Computer Science and Engineering.  Branch Computer Science and Engineering.  Date: 12/12/20  Alm: Javelope a java program to find  |
|       | Branch Computer  |
|       | Date: 12/12/20   |
|       | DIM: java program  |
|       | develope a sinverse)   |
|       | 1 de l'ultiplicative 1 to  |
|       | invelle the respect  |
|       | the under inner  |
|       | is an  |
|       | Branch Computer Screen  Date: 12/12/20  Diff: 12/12/20  To develope a java program to find  Jo develope a java program to find  the invene (Multiplicative invene) of a  munder with respect to  munder multiplicative invene is an  modulus. multiplicative invene is an  |
|       | a modular multiplier a 2 2   |
|       | The work that?   |
|       | given number with respective invent is an and street with and multiplicative invent and multiplicative invent exists if and sometimes in the multiplicative inverse exists if and it are relatively prime.   |
|       | The multiplicative inverse eroists  The prince of the prince |
|       | The multiple relatively 1  |
|       | a au   |
|       | is it a )=1  |
|       | only (a, m) inver  |
|       | only if a & m)=1  gcd (a, m)=1  find the smalliplicative invere  |
|       | find the most them   |
| Maria | (i.e) gcd (a, m)=)  (i.e) gcd (a, m)=)  We can find the knowltiplicative inverse  were can find the knowltiplicative  where c |
|       | We louded the  |
|       | explication  |
|       | uning -  |
|       | Algorithm/ procedure: a and  |
|       | Algorithmy for the two munbels a and   |
|       | Imput the whole whois  |
|       | is the minute  |
|       | Algorithm/procedure:  Algorithm/procedure:  In the number whos  m' where a is the number whos  |
|       | NYVI /O  |

multipliative invent is sequired to find and 'm' is the modulo under which it must be performed. 2) If the two number 'à and 'm' que relatively prime to each other, then a multiplicative inverse exoret 3) If the modulus is 1, then multiplicative invest as o. 4) Vary the extended ecucledean algorithm, the quation is an+1m=1 with the munder in the form of the munder equation (in) 6) place the remainder on the left a = q(m)+1. hard the quotient on the eight hand

2) Duhetstert the number in the Egnation until we get the number whose invesse is required. Jerot Strongh iteps () to ()
untill ged beromes 1. g) Return the multiple of the inverse in the equation which is the inverse 10) terminate the program. Thus Java program to find the Huttiplicative inverse of a given munker with suspect to modulu is implemented and verified.

```
//TO DEVELOP A JAVA PROGRAM TO FIND MODULAR MULTIPLICATIVE INVERSE OF THE GIVEN NUMBER
import java.util.*;
import java.io.*;
class Main{
   public static int gcd(int a, int b)
      if (b == 0)
        return a;
     return gcd(b, a % b);
  public static int modinverse(int a,int m)
    if(gcd(a,m)==1)
    {
    int m0=m;
    int y=0,x=1;
    if(m==1)
       return 0;
    while(a>1 && m!=0)
      int q=a/m;
     int t=m;
     // System.out.println(" "+m);
      m=a%m;
      a=t;
      t=y;
      y=x-q*y;
      x=t;
    }
    if(x<0)
        x+=m0;
    return x;
    }
    else
    {
      return -1;
  public static void main(String args[])
    Scanner sc=new Scanner(System.in);
    System.out.println("Enter the number for which we need to find the multiplicative
inverse");
    int a=sc.nextInt();
    System.out.println("Enter the modulus");
    int m=sc.nextInt();
    int ans=modinverse(a,m);
    if(ans==-1)
        {
```

```
System.out.println("Inverse doesnot exists");
}
else
{
    System.out.println("Modular Multiplicative inverse is:"+modinverse(a,m));
}
}
```

## SAMPLE INPUT/OUTPUT: