Lab4

Shlok Kamath

21BAI1844

Cryptography and Network Security Lab (BCSE309P)

Professor: Dr. RAJESH R

Today's task:

1. Chinese Remainder Theorem
2. Extended Euclidean Algorithm

Chinese Remainder Theorem:

Code:

```
import java.util.*;
public class Main {
    private static int help(int a, int p){
        int[] arr = {0, p, a, 0, 0, 1, 0};
        while(arr[2]!=0){
            arr[0] = arr[1]/arr[2];
            arr[3] = arr[1]%arr[2];
            arr[6] = arr[4] - arr[0]*arr[5];
            arr[1] = arr[2];
            arr[2] = arr[3];
            arr[4] = arr[5];
            arr[5] = arr[6];
        }
        if(arr[4]<0)
            return p+arr[4];
        else
            return arr[4];

    }
    public static void main(String[] args) {
        int[][] arr = {{3,5,0,0}, {1,7,0,0}, {6,8,0,0}}; // Values of
{a,m,M,Minv} for each term

        int M = 1;
        for(int i=0; i<arr.length; i++) M*=arr[i][1];
        for(int i=0; i<arr.length; i++) arr[i][2] = M/arr[i][1];
        for(int i=0; i<arr.length; i++) arr[i][3] = help(arr[i][2],
arr[i][1]);

        int x = 0;
        for(int i=0; i<arr.length; i++) x += arr[i][0]*arr[i][2]*arr[i][3];
        System.out.print(x%M);

    }
}
```

Output:

```
    }
    public static void main(String[] args) {
        int[][] arr = {{3,5,0,0}, {1,7,0,0}, {6,8,0,0}}; // Values of {a,m,M,Minv} for each term

        int M = 1;
        for(int i=0; i<arr.length; i++) M*=arr[i][1];
        for(int i=0; i<arr.length; i++) arr[i][2] = M/arr[i][1];
```

```
Main
C:\Users\kamat\.jdks\openjdk-17.0.2\bin\java.exe "-javaagent:C:\Program Files\JetBrains\IntelliJ ID
78
Process finished with exit code 0
```

Extended Euclidean Algorithm:

```
import java.util.*;
public class Main {
    public static void main(String[] args) {
        int a = 17;
        int p = 43;
        int[] arr = {0, p, a, 0, 0, 1, 0};
        while(arr[2]!=0){
            arr[0] = arr[1]/arr[2];
            arr[3] = arr[1]%arr[2];
            arr[6] = arr[4] - arr[0]*arr[5];
            arr[1] = arr[2];
            arr[2] = arr[3];
            arr[4] = arr[5];
            arr[5] = arr[6];
        }
        if(arr[4]<0)
            System.out.println(p+arr[4]);
        else
            System.out.println(arr[4]);

    }
}
```

Output:

```java
public class Main {
    public static void main(String[] args) {
        int a = 17;
        int p = 43;
        int[] arr = {0, p, a, 0, 0, 1, 0};
        while(arr[2]!=0){
            arr[0] = arr[1]/arr[2];
            arr[3] = arr[1]%arr[2];
            arr[6] = arr[4] - arr[0]*arr[5];
```

Main

```
C:\Users\kamat\.jdks\openjdk-17.0.2\bin\java.exe
38
```