

Lab5

Shlok Kamath

21BAI1844

Cryptography and Network Security Lab (BCSE309P)

Professor: Dr. RAJESH R

Today's task:

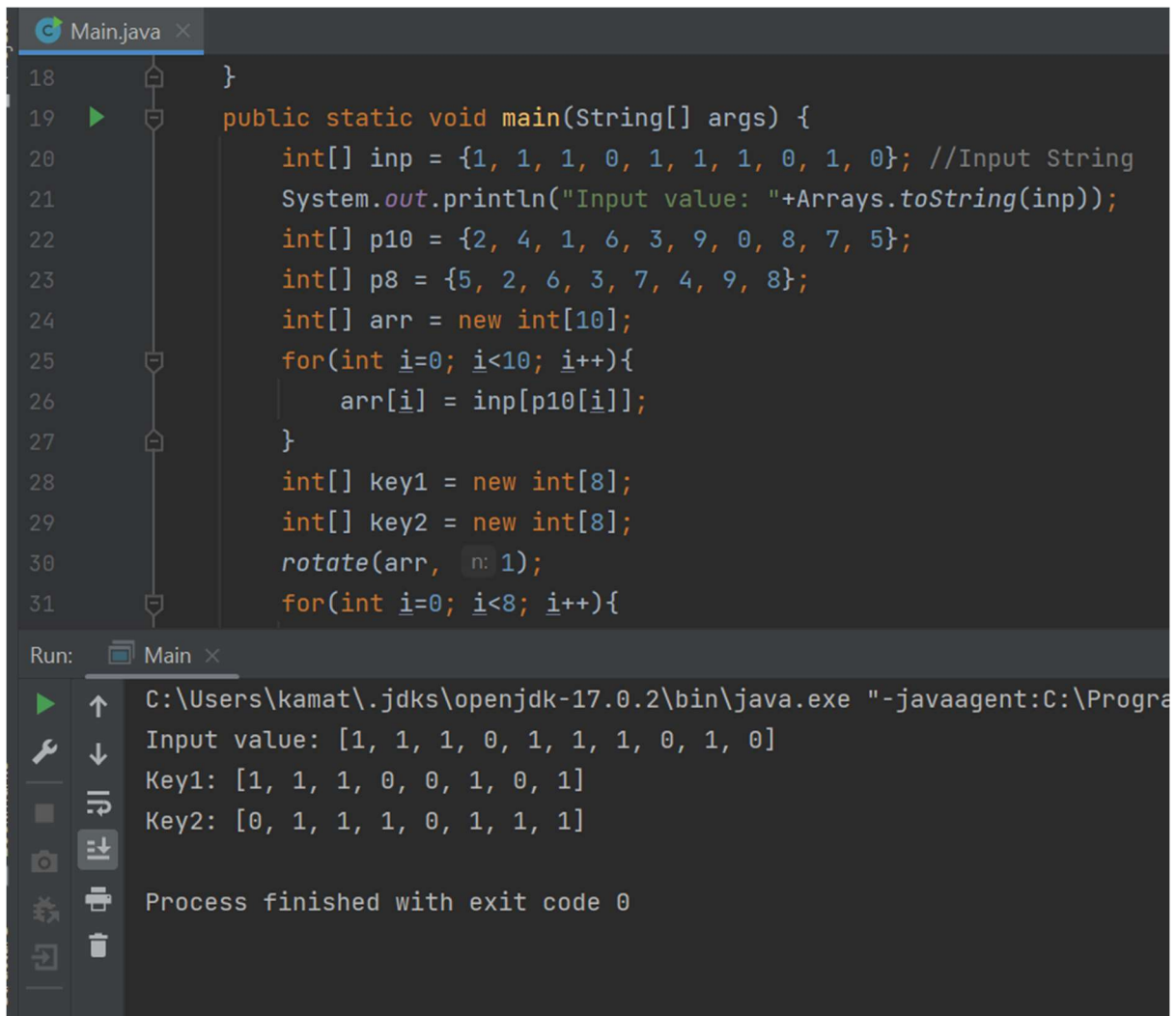
1. Simplified DES

Simplified DES:

Code:

```
import java.util.*;
class Main {
    private static void rotate(int[] arr, int n){
        for(int p=0; p<n; p++){
            int temp = arr[0];
            for(int i=1; i<5; i++){
                arr[i-1] = arr[i];
            }
            arr[4] = temp;
            temp = arr[5];
            for(int i=6; i<10; i++){
                arr[i-1] = arr[i];
            }
            arr[9] = temp;
        }
    }
    public static void main(String[] args) {
        int[] inp = {1, 1, 1, 0, 1, 1, 1, 0, 1, 0}; //Input String
        System.out.println("Input value: "+Arrays.toString(inp));
        int[] p10 = {2, 4, 1, 6, 3, 9, 0, 8, 7, 5};
        int[] p8 = {5, 2, 6, 3, 7, 4, 9, 8};
        int[] arr = new int[10];
        for(int i=0; i<10; i++) arr[i] = inp[p10[i]];
        int[] key1 = new int[8];
        int[] key2 = new int[8];
        rotate(arr, 1);
        for(int i=0; i<8; i++){
            key1[i] = arr[p8[i]];
        }
        rotate(arr, 2);
        for(int i=0; i<8; i++){
            key2[i] = arr[p8[i]];
        }
        System.out.print("Key1: ");
        System.out.println(Arrays.toString(key1));
        System.out.print("Key2: ");
        System.out.println(Arrays.toString(key2));
    }
}
```

Output:



The screenshot shows an IDE with a Java file named 'Main.java'. The code defines a 'main' method that initializes several integer arrays. It prints the 'inp' array, then calculates 'key1' and 'key2' based on the 'inp' array. The 'rotate' method is called on the 'arr' array with a rotation of 1. The output console shows the execution results, including the input array, the calculated keys, and a confirmation that the process finished successfully.

```
18 }
19 public static void main(String[] args) {
20     int[] inp = {1, 1, 1, 0, 1, 1, 1, 0, 1, 0}; //Input String
21     System.out.println("Input value: "+Arrays.toString(inp));
22     int[] p10 = {2, 4, 1, 6, 3, 9, 0, 8, 7, 5};
23     int[] p8 = {5, 2, 6, 3, 7, 4, 9, 8};
24     int[] arr = new int[10];
25     for(int i=0; i<10; i++){
26         arr[i] = inp[p10[i]];
27     }
28     int[] key1 = new int[8];
29     int[] key2 = new int[8];
30     rotate(arr, n: 1);
31     for(int i=0; i<8; i++){
```

Run: Main ×

C:\Users\kamat\.jdk\openjdk-17.0.2\bin\java.exe "-javaagent:C:\Program Files\Java\jdk-17.0.2\bin\javaagent.jar" -Djava.class.path=C:\Users\kamat\.jdk\openjdk-17.0.2\bin\javaagent.jar

Input value: [1, 1, 1, 0, 1, 1, 1, 0, 1, 0]

Key1: [1, 1, 1, 0, 0, 1, 0, 1]

Key2: [0, 1, 1, 1, 0, 1, 1, 1]

Process finished with exit code 0