CRYPTOGRAPHY LABORATORY FILE
CS-511

Submitted to:
Dr. Samayveer Singh
Assistant Professor
Department of Computer Science

Submitted by:
Shashi Shekhar Azad
Roll No.: 23203029
M. Tech. CSE 1st Semester

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DR. B. R. AMBEDKAR NATIONAL INSTITUTE OF TECHNOLOGY
JALANDHAR

Assignment 7

Write a program to implement the encryption and decryption process of RC4.

Code:

```
import java.util.Scanner;
class RC4Algorithm {
    static int[] K = new int[256];
    static int[] S = new int[256];
    static int keylength;
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);
System.out.print("\n==========================RC4Algorithm=======================
==\n");
        System.out.print("\nEnter plain text: ");
        String inpuString = sc.nextLine();
        System.out.print("Enter Key: ");
        String inpuString2 = sc.nextLine();
        char[] plainText = inpuString.toCharArray();
        char[] byteKey = inpuString2.toCharArray();
        initAndPermute(byteKey);
        char[] cipherText = encryptRC4(plainText);
        System.out.print("\nCipher Text: ");
        for (int i = 0; i < cipherText.length; i++) {
            System.out.print(cipherText[i]);
        }
        initAndPermute(byteKey);
        char[] decryptedText = decryptRC4(cipherText);
        System.out.print("\nDecrypted Text: ");
        for (int i = 0; i < decryptedText.length; i++) {
            System.out.print(decryptedText[i]);
        }
System.out.print("\n\n==========================RC4Algorithm=======================
===\n");
        sc.close();
    }
```

```
private static void initAndPermute(char[] byteKey) {
    if (byteKey.length > 256 || byteKey.length < 1) {
        System.out.println("Key length must be between 1 to 256 chars");
    } else {
        // Creation of initial state and key bytes
        keylength = byteKey.length;
        for (int i = 0; i < 256; i++) {
            S[i] = i;
            K[i] = byteKey[i % keylength];
        }
        // Permuting state bytes based on values of key bytes
        int j = 0;
        for (int i = 0; i < 256; i++) {
            j = (j + S[i] + K[i]) % 256;
            int temp = S[i];
            S[i] = S[j];
            S[j] = temp;
        }
    }
}
private static char[] encryptRC4(char[] plainText) {
    char[] cipherText = new char[plainText.length];
    int i = 0;
    int j = 0;
    int key;
    int plainTextLen = 0;
    while (plainTextLen < plainText.length) {
        // Key generation
        i = (i + 1) % 256;
        j = (j + S[i]) % 256;
        int temp = S[i];
        S[i] = S[j];
        S[j] = temp;
        key = S[(S[i] + S[j]) % 256];
        // Encryption
```

```
            cipherText[plainTextLen] = (char) (plainText[plainTextLen] ^ key);
            plainTextLen++;
        }
        return cipherText;
    }
    private static char[] decryptRC4(char[] cipherText) {
        char[] plainText = new char[cipherText.length];
        int i = 0;
        int j = 0;
        int key;
        int cipherLen = 0;
        while (cipherLen < cipherText.length) {
            // Key generation
            i = (i + 1) % 256;
            j = (j + S[i]) % 256;
            int temp = S[i];
            S[i] = S[j];
            S[j] = temp;
            key = S[(S[i] + S[j]) % 256];
            // Encryption
            plainText[cipherLen] = (char) (cipherText[cipherLen] ^ key);
            cipherLen++;
        }
        return plainText;
    }
}
```

Output:

```
==========RC4Algorithm==========

Enter plain text: Hello, This is RC4 Cryptographic Algorithm.
Enter Key: RC4AlgorithmKey

Cipher Text: ???å??éM`<¾á·Ü²??Dö??ÉP?ÿû?û?,¾<??ßrX
Decrypted Text: Hello, This is RC4 Cryptographic Algorithm.

==========RC4Algorithm==========
```