

AIM: To implement RC4 Algorithm

Theory:

RC4 was designed by Ron Rivest. It is based on stream cipher ie the encryption & decryption happens byte by byte. This algorithm generates a random stream of bits known as **keyStream**. This keyStream is combined with plaintext using XOR operation for both encryption & decryption process.

Program

```
import java.security.SecureRandom;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.swing.JOptionPane;
public class RC4Demo
{
    public static void main(String[] args)throws Exception
    {
        String algo="RC4",plain_text,input,key;

        input = JOptionPane.showInputDialog("Input the string to encrypt:");
        key=JOptionPane.showInputDialog("Input the key:");

        SecureRandom sr = new SecureRandom(key.getBytes());
        KeyGenerator kg = KeyGenerator.getInstance(algo);
        kg.init(sr);
        SecretKey sk = kg.generateKey();
        Cipher cipherObj = Cipher.getInstance(algo);
        cipherObj.init(Cipher.ENCRYPT_MODE, sk);
        byte[]encrypt = cipherObj.doFinal(input.getBytes());

        String cipher = new String(encrypt);
        JOptionPane.showMessageDialog (null, "Cipher Text is " + cipher, "Encryption
Process", JOptionPane.PLAIN_MESSAGE);

        Cipher cipherObj1 = Cipher.getInstance(algo);
        cipherObj1.init(Cipher.DECRYPT_MODE, sk);
        byte[] plain = cipherObj1.doFinal(encrypt);
        plain_text = new String(plain);
        System.out.println("Decrypted Text is"+plain_text);
        JOptionPane.showMessageDialog (null, "Plain Text is " + plain_text, "Decryption
Process", JOptionPane.PLAIN_MESSAGE);
    }
}
```