**St. Vincent Pallotti College of Engineering & Technology, Nagpur**
**Department of Computer Engineering**
**Session 2024-25**
**CNS Practical (7th Sem A & B)**
**Practical 7**

**Problem Statement:**

Design and implement a secure and efficient implementation of the RC4 stream cipher method.

**Theory:**

Student need to write the method along with the algorithm and diagram from Forouzan e-book.

**Algorithm:**

```
RC4_Encryption (K)
{
    // Creation of initial state and key bytes
    for (i = 0 to 255)
    {
        S[i] ← i
        K[i] ← Key [i mod KeyLength]
    }
    // Permuting state bytes based on values of key bytes
    j ← 0
    for (i = 0 to 255)
    {
        j ← (j + S[i] + K[i]) mod 256
        swap (S[i] , S[j])
    }
    // Continuously permuting state bytes, generating keys, and encrypting
    i ← 0
    j ← 0
    while (more byte to encrypt)
    {
        i ← (i + 1) mod 256
        j ← (j + S[i]) mod 256
        swap (S [i] , S[j])
        k ← S [(S[i] + S[j]) mod 256]
        // Key is ready, encrypt
        input P
        C ← P ⊕ k
        output C
    }
}
```

**Example:**

1. Let S= [ 0,1,2,3,4,5,6,7], PT = [1,2,2,2] and Key = [5,1,0,1]. Perform the Encryption & Decryption using RC4 method.
2. Class Example.

**Conclusion:**

Students need to write the RC4 analysis for the same.