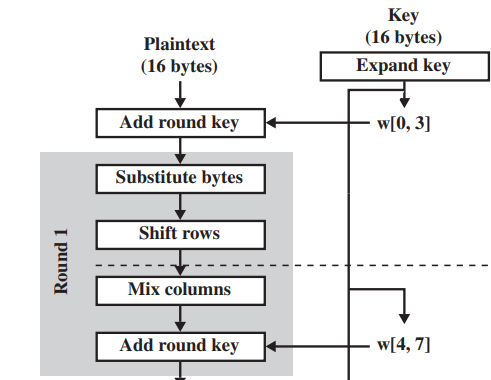
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Course ID** | 108994 | **Course Name** | Cryptography |
| **Date** | 17-03-22 | **Assignment No** | 2 |
|  |  | **Total Points** | 30 |

**Note: Use ASCII scheme for finding decimal equivalents**

Q No 1: Using S-DES Cipher, expand key for 2 rounds and encrypt the PT for only round 1. PT is **L**, key is **a+01**. Show all working. ; 4+6 Pts

Q No 2: Using AES Cipher, expand key for round 1 and encrypt the plaintext for round 1. Follow the following diagram for encryption. PT = **(your full name till 16 characters)** key=**forcesarearrived**. Show all working. 4+10 Pts



Q No 3: Using CBC mode of operation, only encrypt PT **YOU**. Key is **t** and IV is **r**. You will use **AND** operation for encryption. Show all working. 6 Pts