**Marathwada Mitra Mandal’s**

**COLLEGE OF ENGINEERING, PUNE**

**DEPARTMENT OF COMPUTER ENGINEERING**

**BE Comp-II 2020-21**

**SUBJECT: ICS SEMESTER-II**

**Lab Assignment2**

**Implementation of S-AES algorithm**

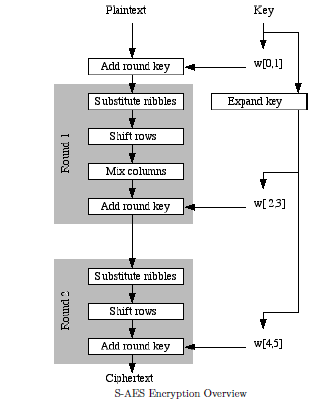
**Group Project by Dibyo and Durvesh**

**Theory:**

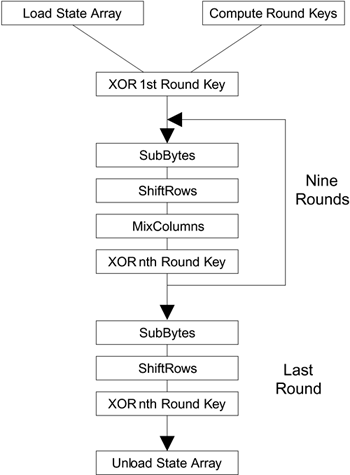
S-AES is to AES as S-DES is to DES. In fact, the structure of S-AES is exactly the same as AES. The

differences are in the key size (16 bits), the block size (16 bits) and the number of rounds (2 rounds). Here is an

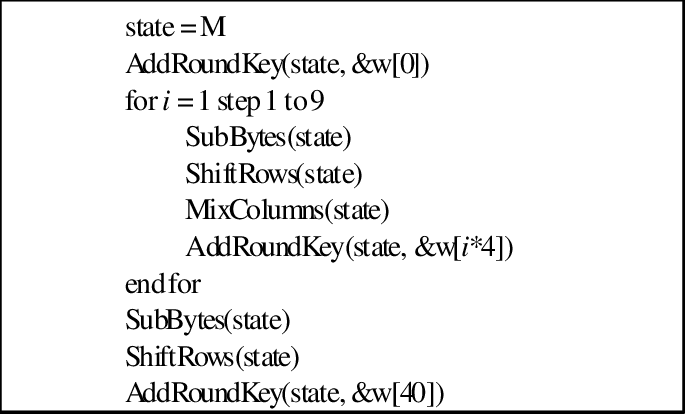
overview:

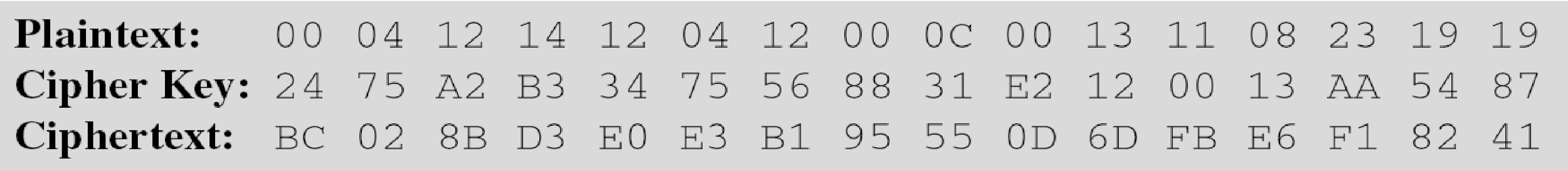


**AES algorithm steps:**

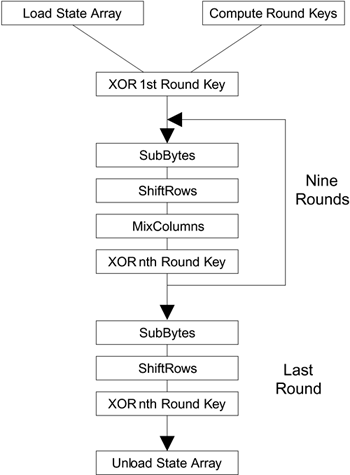


**AES pseudocode for implementation:**





**Implementation steps:**

****

**Result with screenshot:**

**Enter the plaintext :**

**hey,how are you doing?**

**Enter the key :**

**js**

**Cipher text after encryption is :**

**10100100111010000101111010101010100001001110110110011101011111001101101111011011001000100100000101111000010000001001001001001100100011001111110111101000010000101000111000101101**

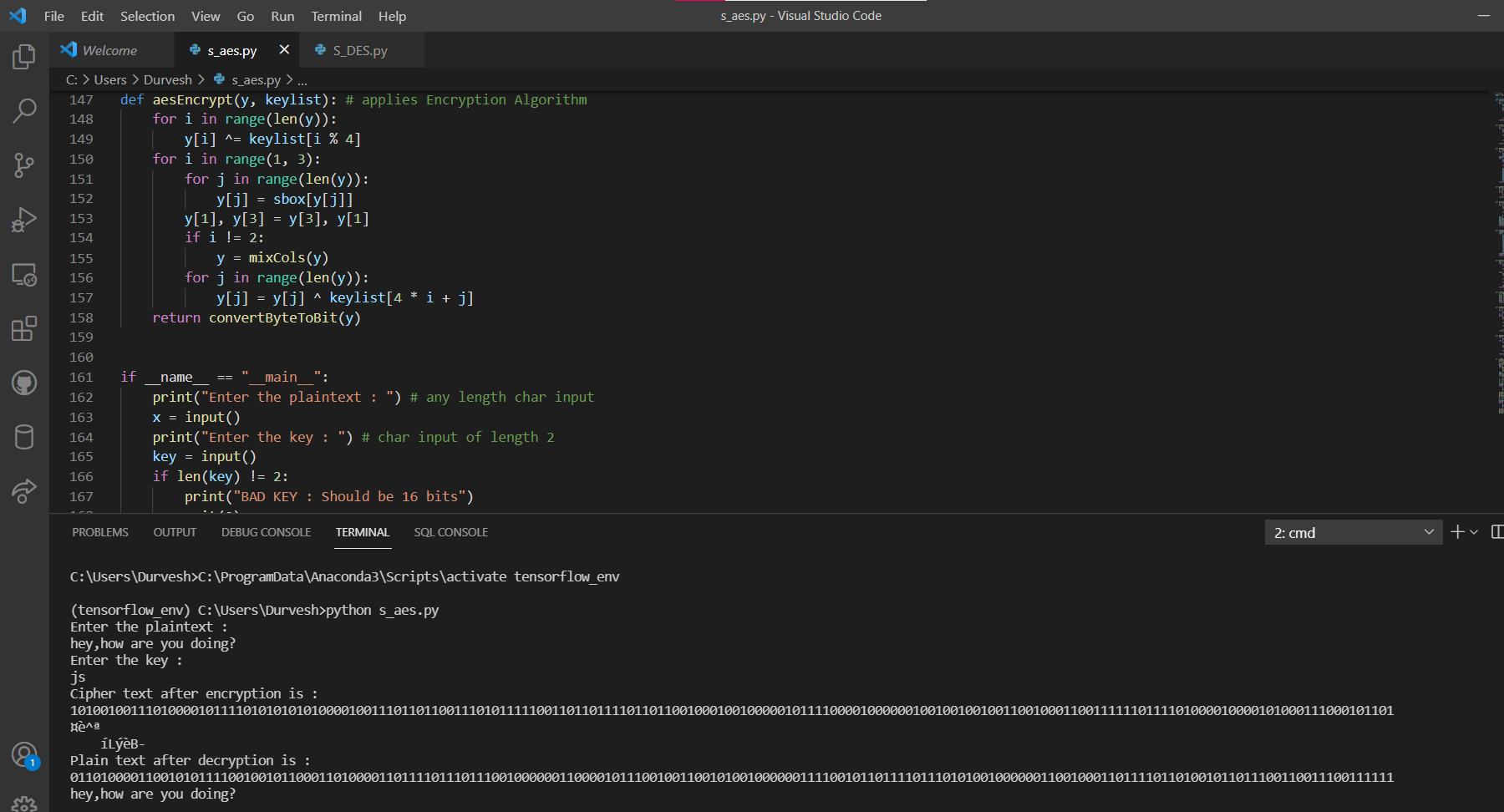
**¤è^ª**

**íLýèB-**

**Plain text after decryption is :**

**01101000011001010111100100101100011010000110111101110111001000000110000101110010011001010010000001111001011011110111010100100000011001000110111101101001011011100110011100111111**

**hey,how are you doing?**

****

**Outcome: Thus the implementation of S-AES algorithm was successfully conducted.**