JSPM’s

JAYWANTRAO SAWANT COLLEGE OF ENGINEERING

Sr.No. 58, Handewadi Road, Hadapsar, Pune, Maharashtra411028 Department of Electronics and Telecommunication Engineering

**EXPERIMENT NO. - 06**

**Name : Pravin Patil**

**Roll No : 3138**

**Program:-**

#include <stdio.h> #include <stdint.h>

#define AES\_BLOCK\_SIZE 16

// ShiftRows: cyclically shift the rows of the state matrix

void ShiftRows(uint8\_t \*state) { uint8\_t temp;

// Second row shift temp = state[1]; state[1] = state[5]; state[5] = state[9]; state[9] = state[13]; state[13] = temp;

// Third row shift temp = state[2]; state[2] = state[10]; state[10] = temp; temp = state[6]; state[6] = state[14]; state[14] = temp;

// Fourth row shift temp = state[3];

state[3] = state[15]; state[15] = state[11]; state[11] = state[7]; state[7] = temp;

}

int main() {

// Example usage of ShiftRows

uint8\_t state[AES\_BLOCK\_SIZE] = {0x32, 0x88, 0x31, 0xe0, 0x43, 0x5a, 0x31, 0x37, 0xf6, 0x30, 0x98, 0x07, 0xa8, 0x8d, 0xa2, 0x34};

printf(" Name:- Yadav Harshdeep Sanjay \n"); printf(" Roll no.:- TE-B 3260 \n");

printf("State Matrix before ShiftRows:\n"); for (int i = 0; i < 4; i++) {

for (int j = 0; j < 4; j++) { printf("%02x ", state[i + 4 \* j]);

}

printf("\n");

}

// ShiftRows operation ShiftRows(state);

printf("\nState Matrix after ShiftRows:\n"); for (int i = 0; i < 4; i++) {

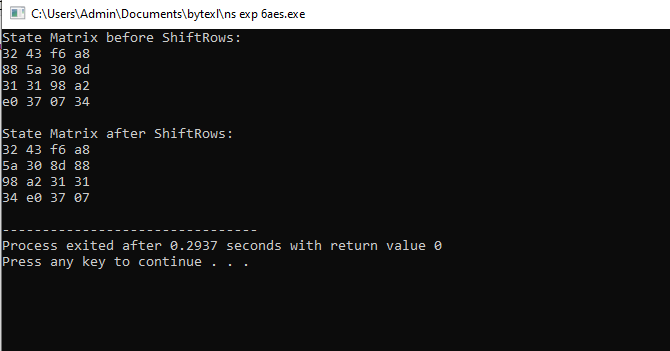
for (int j = 0; j < 4; j++) { printf("%02x ", state[i + 4 \* j]);

}

printf("\n");

}

**Output:-**

****