**Name: Dhanraj Subhash Kore**

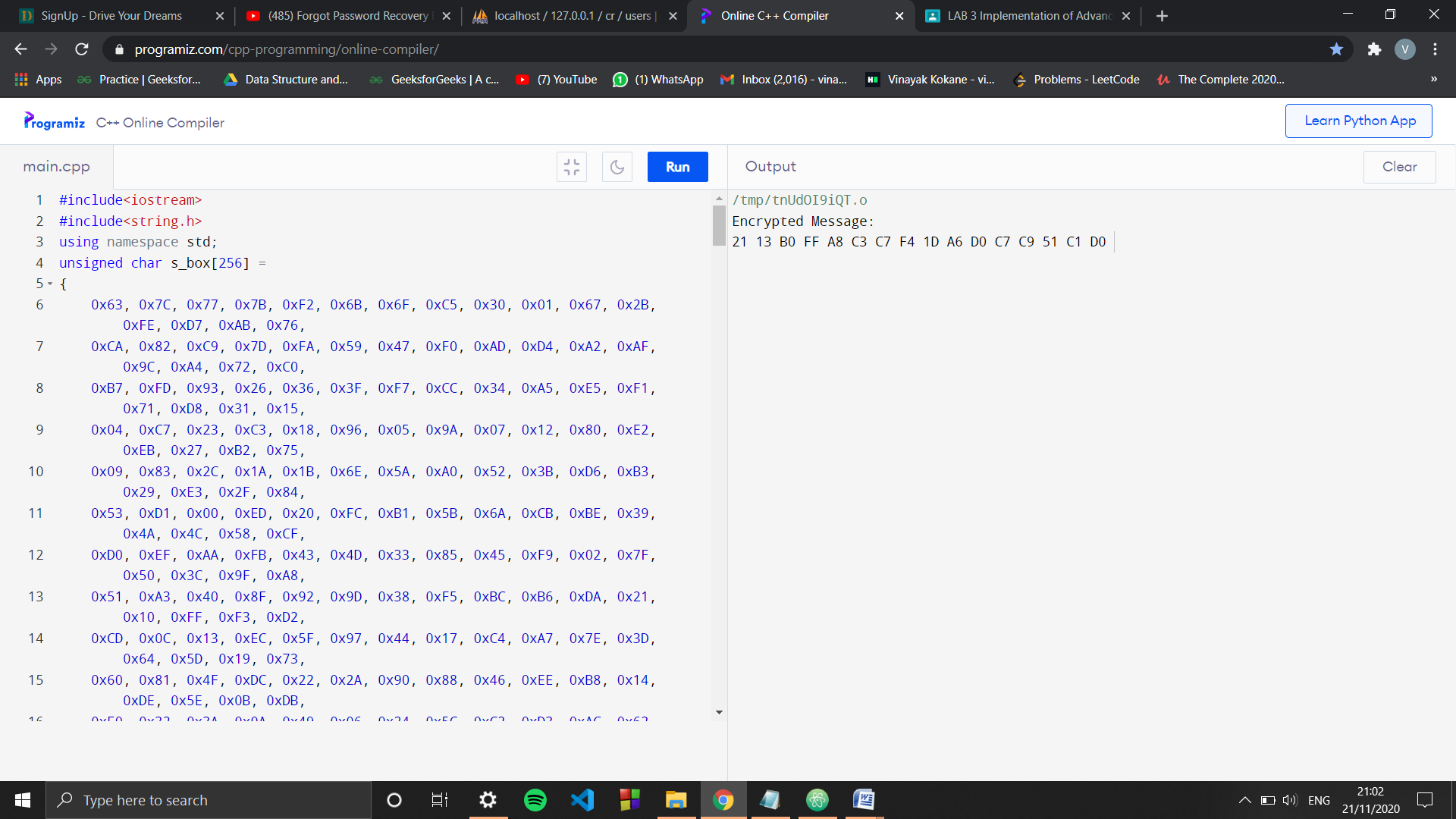
**Div : B Roll No: 60**

**Batch: B-3**

**Sub : CS LAB Assignment**

**LAB 3 Implementation of Advanced Encryption Standard (AES) Algorithm**

**Output screen:**

****

**Code:**

#include<iostream>

#include<string.h>

using namespace std;

unsigned char s\_box[256] =

{

0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76,

0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0,

0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC, 0x34, 0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15,

0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75,

0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84,

0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A, 0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF,

0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D, 0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8,

0x51, 0xA3, 0x40, 0x8F, 0x92, 0x9D, 0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2,

0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73,

0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46, 0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB,

0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06, 0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79,

0xE7, 0xC8, 0x37, 0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08,

0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A,

0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6, 0x0E, 0x61, 0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E,

0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF,

0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16

};

unsigned char mul2[256] =

{

0x00,0x02,0x04,0x06,0x08,0x0a,0x0c,0x0e,0x10,0x12,0x14,0x16,0x18,0x1a,0x1c,0x1e,

0x20,0x22,0x24,0x26,0x28,0x2a,0x2c,0x2e,0x30,0x32,0x34,0x36,0x38,0x3a,0x3c,0x3e,

0x40,0x42,0x44,0x46,0x48,0x4a,0x4c,0x4e,0x50,0x52,0x54,0x56,0x58,0x5a,0x5c,0x5e,

0x60,0x62,0x64,0x66,0x68,0x6a,0x6c,0x6e,0x70,0x72,0x74,0x76,0x78,0x7a,0x7c,0x7e,

0x80,0x82,0x84,0x86,0x88,0x8a,0x8c,0x8e,0x90,0x92,0x94,0x96,0x98,0x9a,0x9c,0x9e,

0xa0,0xa2,0xa4,0xa6,0xa8,0xaa,0xac,0xae,0xb0,0xb2,0xb4,0xb6,0xb8,0xba,0xbc,0xbe,

0xc0,0xc2,0xc4,0xc6,0xc8,0xca,0xcc,0xce,0xd0,0xd2,0xd4,0xd6,0xd8,0xda,0xdc,0xde,

0xe0,0xe2,0xe4,0xe6,0xe8,0xea,0xec,0xee,0xf0,0xf2,0xf4,0xf6,0xf8,0xfa,0xfc,0xfe,

0x1b,0x19,0x1f,0x1d,0x13,0x11,0x17,0x15,0x0b,0x09,0x0f,0x0d,0x03,0x01,0x07,0x05,

0x3b,0x39,0x3f,0x3d,0x33,0x31,0x37,0x35,0x2b,0x29,0x2f,0x2d,0x23,0x21,0x27,0x25,

0x5b,0x59,0x5f,0x5d,0x53,0x51,0x57,0x55,0x4b,0x49,0x4f,0x4d,0x43,0x41,0x47,0x45,

0x7b,0x79,0x7f,0x7d,0x73,0x71,0x77,0x75,0x6b,0x69,0x6f,0x6d,0x63,0x61,0x67,0x65,

0x9b,0x99,0x9f,0x9d,0x93,0x91,0x97,0x95,0x8b,0x89,0x8f,0x8d,0x83,0x81,0x87,0x85,

0xbb,0xb9,0xbf,0xbd,0xb3,0xb1,0xb7,0xb5,0xab,0xa9,0xaf,0xad,0xa3,0xa1,0xa7,0xa5,

0xdb,0xd9,0xdf,0xdd,0xd3,0xd1,0xd7,0xd5,0xcb,0xc9,0xcf,0xcd,0xc3,0xc1,0xc7,0xc5,

0xfb,0xf9,0xff,0xfd,0xf3,0xf1,0xf7,0xf5,0xeb,0xe9,0xef,0xed,0xe3,0xe1,0xe7,0xe5

};

unsigned char mul3[256] =

{

0x00,0x03,0x06,0x05,0x0c,0x0f,0x0a,0x09,0x18,0x1b,0x1e,0x1d,0x14,0x17,0x12,0x11,

0x30,0x33,0x36,0x35,0x3c,0x3f,0x3a,0x39,0x28,0x2b,0x2e,0x2d,0x24,0x27,0x22,0x21,

0x60,0x63,0x66,0x65,0x6c,0x6f,0x6a,0x69,0x78,0x7b,0x7e,0x7d,0x74,0x77,0x72,0x71,

0x50,0x53,0x56,0x55,0x5c,0x5f,0x5a,0x59,0x48,0x4b,0x4e,0x4d,0x44,0x47,0x42,0x41,

0xc0,0xc3,0xc6,0xc5,0xcc,0xcf,0xca,0xc9,0xd8,0xdb,0xde,0xdd,0xd4,0xd7,0xd2,0xd1,

0xf0,0xf3,0xf6,0xf5,0xfc,0xff,0xfa,0xf9,0xe8,0xeb,0xee,0xed,0xe4,0xe7,0xe2,0xe1,

0xa0,0xa3,0xa6,0xa5,0xac,0xaf,0xaa,0xa9,0xb8,0xbb,0xbe,0xbd,0xb4,0xb7,0xb2,0xb1,

0x90,0x93,0x96,0x95,0x9c,0x9f,0x9a,0x99,0x88,0x8b,0x8e,0x8d,0x84,0x87,0x82,0x81,

0x9b,0x98,0x9d,0x9e,0x97,0x94,0x91,0x92,0x83,0x80,0x85,0x86,0x8f,0x8c,0x89,0x8a,

0xab,0xa8,0xad,0xae,0xa7,0xa4,0xa1,0xa2,0xb3,0xb0,0xb5,0xb6,0xbf,0xbc,0xb9,0xba,

0xfb,0xf8,0xfd,0xfe,0xf7,0xf4,0xf1,0xf2,0xe3,0xe0,0xe5,0xe6,0xef,0xec,0xe9,0xea,

0xcb,0xc8,0xcd,0xce,0xc7,0xc4,0xc1,0xc2,0xd3,0xd0,0xd5,0xd6,0xdf,0xdc,0xd9,0xda,

0x5b,0x58,0x5d,0x5e,0x57,0x54,0x51,0x52,0x43,0x40,0x45,0x46,0x4f,0x4c,0x49,0x4a,

0x6b,0x68,0x6d,0x6e,0x67,0x64,0x61,0x62,0x73,0x70,0x75,0x76,0x7f,0x7c,0x79,0x7a,

0x3b,0x38,0x3d,0x3e,0x37,0x34,0x31,0x32,0x23,0x20,0x25,0x26,0x2f,0x2c,0x29,0x2a,

0x0b,0x08,0x0d,0x0e,0x07,0x04,0x01,0x02,0x13,0x10,0x15,0x16,0x1f,0x1c,0x19,0x1a

};

unsigned char rcon[256] = {

0x8d, 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80, 0x1b, 0x36, 0x6c, 0xd8, 0xab, 0x4d, 0x9a,

0x2f, 0x5e, 0xbc, 0x63, 0xc6, 0x97, 0x35, 0x6a, 0xd4, 0xb3, 0x7d, 0xfa, 0xef, 0xc5, 0x91, 0x39,

0x72, 0xe4, 0xd3, 0xbd, 0x61, 0xc2, 0x9f, 0x25, 0x4a, 0x94, 0x33, 0x66, 0xcc, 0x83, 0x1d, 0x3a,

0x74, 0xe8, 0xcb, 0x8d, 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80, 0x1b, 0x36, 0x6c, 0xd8,

0xab, 0x4d, 0x9a, 0x2f, 0x5e, 0xbc, 0x63, 0xc6, 0x97, 0x35, 0x6a, 0xd4, 0xb3, 0x7d, 0xfa, 0xef,

0xc5, 0x91, 0x39, 0x72, 0xe4, 0xd3, 0xbd, 0x61, 0xc2, 0x9f, 0x25, 0x4a, 0x94, 0x33, 0x66, 0xcc,

0x83, 0x1d, 0x3a, 0x74, 0xe8, 0xcb, 0x8d, 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80, 0x1b,

0x36, 0x6c, 0xd8, 0xab, 0x4d, 0x9a, 0x2f, 0x5e, 0xbc, 0x63, 0xc6, 0x97, 0x35, 0x6a, 0xd4, 0xb3,

0x7d, 0xfa, 0xef, 0xc5, 0x91, 0x39, 0x72, 0xe4, 0xd3, 0xbd, 0x61, 0xc2, 0x9f, 0x25, 0x4a, 0x94,

0x33, 0x66, 0xcc, 0x83, 0x1d, 0x3a, 0x74, 0xe8, 0xcb, 0x8d, 0x01, 0x02, 0x04, 0x08, 0x10, 0x20,

0x40, 0x80, 0x1b, 0x36, 0x6c, 0xd8, 0xab, 0x4d, 0x9a, 0x2f, 0x5e, 0xbc, 0x63, 0xc6, 0x97, 0x35,

0x6a, 0xd4, 0xb3, 0x7d, 0xfa, 0xef, 0xc5, 0x91, 0x39, 0x72, 0xe4, 0xd3, 0xbd, 0x61, 0xc2, 0x9f,

0x25, 0x4a, 0x94, 0x33, 0x66, 0xcc, 0x83, 0x1d, 0x3a, 0x74, 0xe8, 0xcb, 0x8d, 0x01, 0x02, 0x04,

0x08, 0x10, 0x20, 0x40, 0x80, 0x1b, 0x36, 0x6c, 0xd8, 0xab, 0x4d, 0x9a, 0x2f, 0x5e, 0xbc, 0x63,

0xc6, 0x97, 0x35, 0x6a, 0xd4, 0xb3, 0x7d, 0xfa, 0xef, 0xc5, 0x91, 0x39, 0x72, 0xe4, 0xd3, 0xbd,

0x61, 0xc2, 0x9f, 0x25, 0x4a, 0x94, 0x33, 0x66, 0xcc, 0x83, 0x1d, 0x3a, 0x74, 0xe8, 0xcb, 0x8d

};

void key\_expansion\_core(unsigned char\* in, unsigned char i)

{

unsigned int \*q = (unsigned int\*) in;

\*q = (\*q >> 8) | ((\*q & 0xff) << 24);

in[0] = s\_box[in[0]];

in[1] = s\_box[in[1]];

in[2] = s\_box[in[2]];

in[3] = s\_box[in[3]];

in[0] ^= rcon[i];

}

void key\_expansion(unsigned char\* input\_key, unsigned char\* expanded\_key){

for(int i = 0;i<16; i++)

expanded\_key[i] = input\_key[i];

int bytes\_generated = 16;

int rcon\_iterations = 1;

unsigned char temp[4];

while(bytes\_generated<176)

{

for(int i=0;i<4;i++)

{

temp[i] = expanded\_key[i + bytes\_generated -4];

}

if(bytes\_generated % 16 == 0)

{

key\_expansion\_core(temp, rcon\_iterations);

rcon\_iterations++;

}

for(unsigned char a=0;a<4;a++)

{

expanded\_key[bytes\_generated] = expanded\_key[bytes\_generated - 16]^temp[a];

bytes\_generated++;

}

}

}

void initial\_round(){ }

void sub\_bytes(unsigned char\* state){

for(int i = 0; i<16; i++)

{

state[i] = s\_box[state[i]];

}

}

void shift\_rows(unsigned char\* state){

unsigned char tmp[16];

tmp[0] = state[0];

tmp[1] = state[5];

tmp[2] = state[10];

tmp[3] = state[15];

tmp[4] = state[4];

tmp[5] = state[9];

tmp[6] = state[14];

tmp[7] = state[3];

tmp[8] = state[8];

tmp[9] = state[13];

tmp[10] = state[2];

tmp[11] = state[7];

tmp[12] = state[12];

tmp[13] = state[1];

tmp[14] = state[6];

tmp[15] = state[11];

for(int i = 0; i<16; i++)

{

state[i] = tmp[i];

}

}

void mix\_columns(unsigned char\* state){

unsigned char tmp[16];

tmp[0] = (unsigned char)(mul2[state[0]]^mul3[state[1]]^state[2]^state[3]);

tmp[1] = (unsigned char)(state[0]^mul2[state[1]]^mul3[state[2]]^state[3]);

tmp[2] = (unsigned char)(state[0]^state[1]^mul2[state[2]]^mul3[state[3]]);

tmp[3] = (unsigned char)(mul3[state[0]]^state[1]^state[2]^mul2[state[3]]);

tmp[4] = (unsigned char)(mul2[state[4]]^mul3[state[5]]^state[6]^state[7]);

tmp[5] = (unsigned char)(state[4]^mul2[state[5]]^mul3[state[6]]^state[7]);

tmp[6] = (unsigned char)(state[4]^state[5]^mul2[state[6]]^mul3[state[7]]);

tmp[7] = (unsigned char)(mul3[state[4]]^state[5]^state[6]^mul2[state[7]]);

tmp[8] = (unsigned char)(mul2[state[8]]^mul3[state[9]]^state[10]^state[11]);

tmp[9] = (unsigned char)(state[8]^mul2[state[9]]^mul3[state[10]]^state[11]);

tmp[10] = (unsigned char)(state[8]^state[9]^mul2[state[10]]^mul3[state[11]]);

tmp[11] = (unsigned char)(mul3[state[8]]^state[9]^state[10]^mul2[state[11]]);

tmp[12] = (unsigned char)(mul2[state[12]]^mul3[state[13]]^state[14]^state[15]);

tmp[13] = (unsigned char)(state[12]^mul2[state[13]]^mul3[state[14]]^state[15]);

tmp[14] = (unsigned char)(state[12]^state[13]^mul2[state[14]]^mul3[state[15]]);

tmp[15] = (unsigned char)(mul3[state[12]]^state[13]^state[14]^mul2[state[15]]);

for(int i = 0; i<16; i++)

{

state[i] = tmp[i];

}

}

void add\_round\_keys(unsigned char\* state, unsigned char\* round\_key){

for(int i=0;i<16;i++)

{

state[i] ^= round\_key[i];

}

}

void AES\_encrypt(unsigned char\* message, unsigned char\* key)

{

int nor = 9;

unsigned char state[16];

unsigned char expanded\_key[176];

for(int i = 0;i<16;i++)

state[i] = message[i];

key\_expansion(key, expanded\_key);

add\_round\_keys(state, key);

for(int i= 0; i<nor; i++)

{

sub\_bytes(state);

shift\_rows(state);

mix\_columns(state);

add\_round\_keys(state, expanded\_key + (16\*(i+1)));

}

/\*The Final Round\*/

sub\_bytes(state);

shift\_rows(state);

add\_round\_keys(state, expanded\_key + 160);

for(int i=0;i<16;i++)

message[i] = state[i];

}

void print\_hex(unsigned char x)

{

if(x/16 < 10) cout<<(char)((x/16) + '0');

if(x/16 >= 10) cout<<(char)((x/16 - 10) + 'A');

if(x%16 < 10) cout<<(char)((x%16) + '0');

if(x%16 >= 10) cout<<(char)((x%16 - 10) + 'A');

}

int main()

{

unsigned char msg[] = "Facebook";

unsigned char key[16] = {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16};

int original\_len = strlen((const char \*)msg);

int padded\_len = original\_len;

if(padded\_len % 16 != 0)

{

padded\_len = (padded\_len / 16 + 1) \* 16;

}

unsigned char\* padded\_msg = new unsigned char[padded\_len];

for (int i=0;i<padded\_len;i++)

{

if(i > original\_len)

padded\_msg[i] = 0;

else

padded\_msg[i] = msg[i];

}

for(int i = 0; i<padded\_len; i+=16)

{

AES\_encrypt(padded\_msg + i, key);

}

cout<<"Encrypted Message:"<<endl;

for(int i = 0; i< padded\_len; i++)

{

print\_hex(padded\_msg[i]);

cout<<" ";

}

delete[] padded\_msg;

return 0;

}