

```

1  #include <stdio.h>
2  #include "prototypes.h"
3
4
5  int main(void)
6  {
7
8  #if DEMO
9      /* Data from project demo for testing*/
10     unsigned char input[16] = { 0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77,
11                                0x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff };
12     unsigned char key[256] = { 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
13                                0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };
14     char * sbboxType = "original";
15 #else
16     unsigned char input[16] = { 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
17                                0x00, 0x00, 0x00, 0x00, 0xab, 0xd1 };
18     unsigned char key[256] = { 0x1a, 0x0c, 0x24, 0xf2, 0x87, 0x54, 0x93, 0xbc,
19                                0xb7, 0x08, 0x0e, 0x43, 0x93, 0x0f, 0x56, 0x81 };
20     char * sbboxType = "modified";
21 #endif
22
23     printf("\n\n-----\n\n");
24     printf("ID1 = 104 337 378  (Jason Choquette) \n");
25     printf("ID2 = 103 385 550  (Yu Sheng Tian) \n");
26     printf("Group Code (J, Y)= (3,7) \n\n\n");
27     printf("Assigned Plaintext and Key:\n");
28     printf("\t");
29     for (int i = 0; i < 16; i++)
30         printf("%02x ", input[i]);
31
32     printf("\n\t");
33     for (int i = 0; i < 16; i++)
34         printf("%02x ", key[i]);
35
36     printf("\n\n\n");
37     printf("-----\n");
38     printf("Key Schedule Results for Each Round with the %s AES:\n", sbboxType);
39     printf("-----\n");
40
41     print_expand_key(key);
42
43     printf("\n\n");
44     printf("-----\n");
45     printf("Data Results for Each Round with the %s AES:\n", sbboxType);
46     printf("-----\n");
47
48     AesEncrypt(input, key, 10);
49
50     getchar();
51     return 0;

```

49 }

50

51