```
 1 /*
 2  * The MIT License (MIT)
 3  *
 4  * Copyright (c) 2018 Zhou Zhi Gang
 5  * Email: keorapetse.finger@yahoo.com
 6  *
 7  * Permission is hereby granted, free of charge, to any person obtaining a copy
 8  * of this software and associated documentation files (the "Software"), to
   deal
 9  * in the Software without restriction, including without limitation the rights
10  * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
11  * copies of the Software, and to permit persons to whom the Software is
12  * furnished to do so, subject to the following conditions:
13  *
14  * The above copyright notice and this permission notice shall be included in
15  * all copies or substantial portions of the Software.
16  *
17  * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
18  * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
19  * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
20  * AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
21  * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM
   ,
22  * OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
23  * THE SOFTWARE.
24  */
25 #ifndef __TABLES__H
26 #define __TABLES__H
27
28 /* The MDS Matrix */
29 uint8_t mds[4][4]=
30 {
31     {0x01, 0xef, 0x5b, 0x5b},
32     {0x5b, 0xef, 0xef, 0x01},
33     {0xef, 0x5b, 0x01, 0xef},
34     {0xef, 0x01, 0xef, 0x5b}
35 };
36
37 /*
38  * The Permutations q0 and q1 The permutations q0 and q1 are □xed permutations
   on
39  * 8-bit values. They are constructed from four di□erent 4-bit permutations
   each.
40  * We ha ve in vestigated the resulting 8-bit permutations, q0 and q1,
   extensively,
41  * and believe them to be at least no weaker than randomly selected 8-bit
   permutations.
42  */
43 uint8_t q[2][256] =
44 {
45     /* q0 */
46     {
47         0xa9, 0x67, 0xb3, 0xe8, 0x04, 0xfd, 0xa3, 0x76, 0x9a, 0x92, 0x80, 0x78,
    0xe4, 0xdd, 0xd1, 0x38,
48         0x0d, 0xc6, 0x35, 0x98, 0x18, 0xf7, 0xec, 0x6c, 0x43, 0x75, 0x37, 0x26,
    0xfa, 0x13, 0x94, 0x48,
49         0xf2, 0xd0, 0x8b, 0x30, 0x84, 0x54, 0xdf, 0x23, 0x19, 0x5b, 0x3d, 0x59,
    0xf3, 0xae, 0xa2, 0x82,
50         0x63, 0x01, 0x83, 0x2e, 0xd9, 0x51, 0x9b, 0x7c, 0xa6, 0xeb, 0xa5, 0xbe,
    0x16, 0x0c, 0xe3, 0x61,
51         0xc0, 0x8c, 0x3a, 0xf5, 0x73, 0x2c, 0x25, 0x0b, 0xbb, 0x4e, 0x89, 0x6b,
    0x53, 0x6a, 0xb4, 0xf1,
52         0xe1, 0xe6, 0xbd, 0x45, 0xe2, 0xf4, 0xb6, 0x66, 0xcc, 0x95, 0x03, 0x56,
    0xd4, 0x1c, 0x1e, 0xd7,
53         0xfb, 0xc3, 0x8e, 0xb5, 0xe9, 0xcf, 0xbf, 0xba, 0xea, 0x77, 0x39, 0xaf,
    0x33, 0xc9, 0x62, 0x71,
54         0x81, 0x79, 0x09, 0xad, 0x24, 0xcd, 0xf9, 0xd8, 0xe5, 0xc5, 0xb9, 0x4d,
    0x44, 0x08, 0x86, 0xe7,
55         0xa1, 0x1d, 0xaa, 0xed, 0x06, 0x70, 0xb2, 0xd2, 0x41, 0x7b, 0xa0, 0x11,
    0x31, 0xc2, 0x27, 0x90,
```

```
56          0x20, 0xf6, 0x60, 0xff, 0x96, 0x5c, 0xb1, 0xab, 0x9e, 0x9c, 0x52, 0x1b
   , 0x5f, 0x93, 0x0a, 0xef,
57          0x91, 0x85, 0x49, 0xee, 0x2d, 0x4f, 0x8f, 0x3b, 0x47, 0x87, 0x6d, 0x46
   , 0xd6, 0x3e, 0x69, 0x64,
58          0x2a, 0xce, 0xcb, 0x2f, 0xfc, 0x97, 0x05, 0x7a, 0xac, 0x7f, 0xd5, 0x1a
   , 0x4b, 0x0e, 0xa7, 0x5a,
59          0x28, 0x14, 0x3f, 0x29, 0x88, 0x3c, 0x4c, 0x02, 0xb8, 0xda, 0xb0, 0x17
   , 0x55, 0x1f, 0x8a, 0x7d,
60          0x57, 0xc7, 0x8d, 0x74, 0xb7, 0xc4, 0x9f, 0x72, 0x7e, 0x15, 0x22, 0x12
   , 0x58, 0x07, 0x99, 0x34,
61          0x6e, 0x50, 0xde, 0x68, 0x65, 0xbc, 0xdb, 0xf8, 0xc8, 0xa8, 0x2b, 0x40
   , 0xdc, 0xfe, 0x32, 0xa4,
62          0xca, 0x10, 0x21, 0xf0, 0xd3, 0x5d, 0x0f, 0x00, 0x6f, 0x9d, 0x36, 0x42
   , 0x4a, 0x5e, 0xc1, 0xe0
63      },
64      /* q1 */
65      {
66          0x75, 0xf3, 0xc6, 0xf4, 0xdb, 0x7b, 0xfb, 0xc8, 0x4a, 0xd3, 0xe6, 0x6b
   , 0x45, 0x7d, 0xe8, 0x4b,
67          0xd6, 0x32, 0xd8, 0xfd, 0x37, 0x71, 0xf1, 0xe1, 0x30, 0x0f, 0xf8, 0x1b
   , 0x87, 0xfa, 0x06, 0x3f,
68          0x5e, 0xba, 0xae, 0x5b, 0x8a, 0x00, 0xbc, 0x9d, 0x6d, 0xc1, 0xb1, 0x0e
   , 0x80, 0x5d, 0xd2, 0xd5,
69          0xa0, 0x84, 0x07, 0x14, 0xb5, 0x90, 0x2c, 0xa3, 0xb2, 0x73, 0x4c, 0x54
   , 0x92, 0x74, 0x36, 0x51,
70          0x38, 0xb0, 0xbd, 0x5a, 0xfc, 0x60, 0x62, 0x96, 0x6c, 0x42, 0xf7, 0x10
   , 0x7c, 0x28, 0x27, 0x8c,
71          0x13, 0x95, 0x9c, 0xc7, 0x24, 0x46, 0x3b, 0x70, 0xca, 0xe3, 0x85, 0xcb
   , 0x11, 0xd0, 0x93, 0xb8,
72          0xa6, 0x83, 0x20, 0xff, 0x9f, 0x77, 0xc3, 0xcc, 0x03, 0x6f, 0x08, 0xbf
   , 0x40, 0xe7, 0x2b, 0xe2,
73          0x79, 0x0c, 0xaa, 0x82, 0x41, 0x3a, 0xea, 0xb9, 0xe4, 0x9a, 0xa4, 0x97
   , 0x7e, 0xda, 0x7a, 0x17,
74          0x66, 0x94, 0xa1, 0x1d, 0x3d, 0xf0, 0xde, 0xb3, 0x0b, 0x72, 0xa7, 0x1c
   , 0xef, 0xd1, 0x53, 0x3e,
75          0x8f, 0x33, 0x26, 0x5f, 0xec, 0x76, 0x2a, 0x49, 0x81, 0x88, 0xee, 0x21
   , 0xc4, 0x1a, 0xeb, 0xd9,
76          0xc5, 0x39, 0x99, 0xcd, 0xad, 0x31, 0x8b, 0x01, 0x18, 0x23, 0xdd, 0x1f
   , 0x4e, 0x2d, 0xf9, 0x48,
77          0x4f, 0xf2, 0x65, 0x8e, 0x78, 0x5c, 0x58, 0x19, 0x8d, 0xe5, 0x98, 0x57
   , 0x67, 0x7f, 0x05, 0x64,
78          0xaf, 0x63, 0xb6, 0xfe, 0xf5, 0xb7, 0x3c, 0xa5, 0xce, 0xe9, 0x68, 0x44
   , 0xe0, 0x4d, 0x43, 0x69,
79          0x29, 0x2e, 0xac, 0x15, 0x59, 0xa8, 0x0a, 0x9e, 0x6e, 0x47, 0xdf, 0x34
   , 0x35, 0x6a, 0xcf, 0xdc,
80          0x22, 0xc9, 0xc0, 0x9b, 0x89, 0xd4, 0xed, 0xab, 0x12, 0xa2, 0x0d, 0x52
   , 0xbb, 0x02, 0x2f, 0xa9,
81          0xd7, 0x61, 0x1e, 0xb4, 0x50, 0x04, 0xf6, 0xc2, 0x16, 0x25, 0x86, 0x56
   , 0x55, 0x09, 0xbe, 0x91
82      },
83  };
84
85  #endif
86
```