```
# -*- coding: utf-8 -*-
#
# The MIT License (MIT)
#
# Copyright (c) 2018 Zhou Zhi Gang
# Email: keorapetse.finger@yahoo.com
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
# THE SOFTWARE.
#

header ='''
/*
 * The MIT License (MIT)
 *
 * Copyright (c) 2018 Zhou Zhi Gang
 * Email: keorapetse.finger@yahoo.com
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy
 * of this software and associated documentation files (the "Software"), to
deal
 * in the Software without restriction, including without limitation the rights
 * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
 * copies of the Software, and to permit persons to whom the Software is
 * furnished to do so, subject to the following conditions:
 *
 * The above copyright notice and this permission notice shall be included in
 * all copies or substantial portions of the Software.
 *
 * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
 * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
 * AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
 * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM
,
 * OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
 * THE SOFTWARE.
 */
 #ifndef __TABLES__H
 #define __TABLES__H

 /* The MDS Matrix */
 uint8_t mds[4][4]=
 {
    {0x01, 0xef, 0x5b, 0x5b},
    {0x5b, 0xef, 0xef, 0x01},
    {0xef, 0x5b, 0x01, 0xef},
    {0xef, 0x01, 0xef, 0x5b}
 };

 /*
 * The Permutations q0 and q1 The permutations q0 and q1 are □xed permutations
on
 * 8-bit values. They are constructed from four di□erent 4-bit permutations
each.
```

```
 67  * We ha ve in vestigated the resulting 8-bit permutations, q0 and q1,
    extensively,
 68  * and believe them to be at least no weaker than randomly selected 8-bit
    permutations.
 69  */
 70
 71  '''
 72
 73 upper_body = '''
 74 uint8_t q[2][256] =
 75 {
 76     /* q0 */
 77     {
 78         '''
 79 lower_body = '''
 80     /* q1 */
 81     {
 82 '''
 83
 84 footer = '''
 85 };
 86
 87 #endif
 88 '''
 89
 90 path = "./include/tables.h"
 91
 92 # s-box 1
 93 q0 =[
 94     [0x8,0x1,0x7,0xD,0x6,0xF,0x3,0x2,0x0,0xB,0x5,0x9,0xE,0xC,0xA,0x4],
 95     [0xE,0xC,0xB,0x8,0x1,0x2,0x3,0x5,0xF,0x4,0xA,0x6,0x7,0x0,0x9,0xD],
 96     [0xB,0xA,0x5,0xE,0x6,0xD,0x9,0x0,0xC,0x8,0xF,0x3,0x2,0x4,0x7,0x1],
 97     [0xD,0x7,0xF,0x4,0x1,0x2,0x6,0xE,0x9,0xB,0x3,0x0,0x8,0x5,0xC,0xA]
 98 ]
 99
100 # s-box 2
101 q1 =[
102     [0x2,0x8,0xB,0xD,0xF,0x7,0x6,0xE,0x3,0x1,0x9,0x4,0x0,0xA,0xC,0x5],
103     [0x1,0xE,0x2,0xB,0x4,0xC,0x3,0x7,0x6,0xD,0xA,0x5,0xF,0x9,0x0,0x8],
104     [0x4,0xC,0x7,0x5,0x1,0x6,0x9,0xA,0x0,0xE,0xD,0x8,0x2,0xB,0x3,0xF],
105     [0xB,0x9,0x5,0x1,0xC,0x3,0xD,0xE,0x6,0x4,0x7,0xF,0x2,0x0,0x8,0xA]
106 ]
107
108 # Rotate a 4-bit nibble
109 def ror(a,b):
110     return (((a>>b)&0xf)|((a<<(4-b))&0xf))
111
112 # Left-shift a 4-bit nibble
113 def lsh(a,b):
114     return ((a<<b)&0xf)
115
116 # Derives a and b from previous paramters
117 def h(a,b):
118     a1 = a^b
119     b1 = a^ror(b,1)^lsh(a,3)
120     return (a1,b1)
121
122 # Generate permutation value
123 def permute(q,x):
124     '''
125     The permutations q0 and q1 are fixed permutations on 8-bit values.
126     They are constructed from four different 4-bit permutations each.
127     For the input value x, we define the corresponding output value y.
128     '''
129     a0,b0 = ((x>>4)&0xf),(x&0xf)
130     a1,b1 = h(a0,b0)
131     a2,b2 = q[0][a1],q[1][b1]
132     a3,b3 = h(a2,b2)
133     a4,b4 = q[2][a3],q[3][b3]
134     return ((b4<<4|a4)&0xff)
```

```
135
136 def write_body(q,t):
137     for x in range(255):
138         y = permute(q,x)
139         if x%16 == 0:
140             t.write("\n\t\t0x%x," % y)
141         else:
142             t.write("0x%x," % y)
143     t.write("0x%x" % permute(q,255))
144     pass
145
146 if __name__ == "__main__":
147     t = open(path,"w+")
148     t.write(header)
149     t.write(upper_body)
150     write_body(q0,t)
151     t.write('''\n\t},''')
152     t.write(lower_body)
153     write_body(q1,t)
154     t.write('''\n\t}''')
155     t.write(footer)
156     t.close()
157     pass
158
159
```