

```

1  /*****
2  *   FILE: SDESConstants
3  *   AUTHOR: Connor Beardsmore - 15504319
4  *   UNIT: FCC200
5  *   PURPOSE: Structures to represent the constants in the SDES algorithm
6  *   LAST MOD: 21/03/17
7  *   REQUIRES: NONE
8  *****/
9
10 public class SDESConstants
11 {
12     // P10 PERMUTATION FOR THE 10-BIT KEY
13     public static final int[] P10 = { 2, 4, 1, 6, 3, 9, 0, 8, 7, 5 };
14
15     //-----
16
17     // P8 PERMUTATION FOR THE 10-BIT KEY
18     public static final int[] P8 = { 5, 2, 6, 3, 7, 4, 9, 8 };
19
20     //-----
21
22     // INITIAL PERMUTATION FOR THE 8-BIT PLAINTEXT
23     public static final int[] IP = { 1, 5, 2, 0, 3, 7, 4, 6 };
24
25     //-----
26
27     // INVERSE PERMUTATION FOR THE 8-BIT PLAINTEXT
28     public static final int[] IPI = { 3, 0, 2, 4, 6, 1, 7, 5 };
29
30     //-----
31
32     // EXPANSION PERMUTATION FOR 4-BITS IN Fk
33     public static final int[] EP = { 3, 0, 1, 2, 1, 2, 3, 0 };
34
35     //-----
36
37     // P4 PERMUTATION AFTER THE S-BOX SELECTION
38     public static final int[] P4 = { 1, 3, 2, 0 };
39
40     //-----
41
42     // SBOX ONE
43     public static final int[][] S0 = { { 1, 0, 3, 2 },
44                                         { 3, 2, 1, 0 },
45                                         { 0, 2, 1, 3 },
46                                         { 3, 1, 3, 2 } };
47
48     //-----
49
50     // SBOX TWO
51     public static final int[][] S1 = { { 0, 1, 2, 3 },
52                                         { 2, 0, 1, 3 },
53                                         { 3, 0, 1, 0 },
54                                         { 2, 1, 0, 3 } };
55
56     //-----
57 }
58

```