CS 153: Introduction to Computer Security

Machine Problem 1: SmallDES

Directions:

- Create a program that will solve the problem below.
- The program must written in the C programming language, using only the following libraries stdio.h, stdlib.h, string.h
- The program must compile using standard Linux GCC (Ubuntu 16.04)
- Input file must be named mp1.txt
- Input must follow the sample input
- Source Code: (smalldes201512345.c)
- Source Code: (breaker201512345.c)
- Zip your source code, then use the following file name: <studentnumber>.zip
- Output file must be named <studentnumber>.txt (i.e 201512345.txt)
- Email to: profmr.profmrs.z@gmail.com
- Output file must be of the same format as the one shown in the sample output
- The following are not allowed:
  - Discussing of the MP outside of class.
  - Downloading code from the internet
  - Copying from your classmate
  - Using your classmate/someone else's source code
- MP Deadline: March 4, 2017 – 5:00 PM.

Title: SmallDES

A SmallDES algorithm is designed similarly with DES, with some small modifications.

1) The SmallDES program takes in a 16 bit input, and a 12 bit key.
2) An initial permutation step is done on the input text using the following permutation matrix

10	3	4	5	9	11	13	1	6	16	2	14	8	15	7	12
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*

3) Divide the resulting text into two equal parts: left part (L_0) and right part (R_0)
4) The Feistel iteration will be done as follows:
   a. $L_i = R_{i-1}$
   b. $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

   There will be 4 rounds of the Feistel iteration
5) The round function $f(R_{i-1}, K_i)$ is defined as follows
   a. Expansion step: R_{i-1} will be divided into four groups of two bits each:

1		2		3		4		5		6		7		8	
8	1	2	3	2	3	4	5	4	5	6	7	6	7	8	1

   b. XOR the resulting expansion sequence with K_i (as based from key schedule).
   c. S-box substitution step: The following will be the S boxes for each of

   S-box 1:

		MIDDLE BITS

		00	01	10	11
OUTER BITS	00	0000	0001	0010	0011
	01	0100	0101	0110	0111
	10	1000	1001	1010	1011
	11	1100	1101	1110	1111

S-box 2:

		MIDDLE BITS			
		00	01	10	11
OUTER BITS	00	0000	1000	0001	1001
	01	0100	1100	0100	1100
	10	0010	1010	1010	1011
	11	0110	1100	0111	1111

S-box 3:

		MIDDLE BITS			
		00	01	10	11
OUTER BITS	00	0000	0100	0010	0110
	01	0001	0101	0011	0111
	10	1000	1100	1010	1110
	11	1001	1101	1011	1111

S-box 4:

		MIDDLE BITS			
		00	01	10	11
OUTER BITS	00	0000	0100	0010	0110
	01	1000	1010	1100	1110
	10	0001	0011	0101	0111
	11	1001	1011	1101	1111

d. Inverse Expansion: For each of the 4 bit output of the S - boxes, remove the two outer bits to obtain 4 groups of two bits each .

e. Permutation box: Use the following permutation, to permute the elements of the current value of R_{i-1}

3	5	8	6	2	4	1	7

f. XOR the result with L_{i-1}

6) After 4 rounds, concatenate L_i and R_i perform inverse permutation

8	11	2	3	4	9	15	13	5	1	6	16	7	12	14	10
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*

7) The result after the inverse permutation step (IP^{-1}) will be the algorithms' final result.

8) Key schedule: Given a 12 bit key, the following will be the result of the key that will be used in the subsequent subkeys

key	1	2	3	4	5	6	7	8	9	10	11	12				
K_1	1	2	3	1	4	5	6	2	7	8	9	3	10	11	12	4
K_2	1	2	3	2	4	5	6	4	7	8	9	6	10	11	12	8
K_3	1	2	3	3	4	5	6	6	7	8	9	9	10	11	12	12
K_4	1	2	3	4	4	5	6	8	7	8	9	12	10	11	12	4

The SmallDES algorithm is a useful symmetric algorithm, however it has been altered using your student numbers.

The following has areas has been altered

1) Two of IP values has been changed.
2) The sequence of S-boxes has been changed.
3) Two P-box values has been changed
4) Two of the IP^{-1} values has been modified.

Goal: Program SmallDES with the alterations that will produce the output text that were provided to you.

By submitting your MP you are acknowledging the following:

1) You didn’t download any piece of code from the internet
2) You didn’t share any of your code to your classmate
3) You didn’t use any piece of code from your classmate