2 Simplified Block Cipher (Max 10pts)

This problem refers to Simplified Block Cipher, described in the file 'Simplified Block Cipher.pdf'. Especially go through examples of encryption and decryption.

Using Simplified Block Cipher, decrypt the string (10100010) using the key (0111111101) by hand ("pen & paper").

Report the whole walkthrough bit by bit with intermediate results after each function (IP, first f_k, SW, second f_k, IP^{-1}).

Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2
(i.e., A = 0000, B = 0001, ..., P = 1111).
Hint: As a midway check, after the application of SW, the string should be (00010011) and one of the decoded letters is 'K'.

String(ciphertext):	10100010		
Key:	0111111101		
Calculating k1 and k2			
p10 used bits	0111111101		
p10 result	1111110011		
LS-1 input	11111	LS-1	10011
LS-1 result	11111		00111
p8 used bits	1111100111		
p8 result=key 1	01011111		
LS-2 input	11111	LS-2	00111
LS-2 result	11111		11100
p8 used bits	1111111100		
p8 result=key 2	11111100		

decryption

String(ciphertext):	10100010	
key 1	01011111	
key 2	11111100	
ip(ciphertext) input	10100010	
ip(ciphertext) result	00110001	
L	0011	
R	0001	
SK	11111100	
E/P input	0001	
E/P result	10000010	
XOR input	10000010,	11111100
XOR result	01111110	
s0 input	0111	
s0 array	1032	
	3210	
	0213	
	3132	
s0row result	dec(1)	
s0column result	dec(3)	
s0bin result	00	
s1 input	1110	
s1 array	0123	
	2013	
	3010	
	2103	
s1row result	dec(2)	
s1column result	dec(3)	
s1bin result	00	
s0+s1 result	0000	
p4 input	0000	
p4 result	0000	
XOR (L, p4 result)	0011	0000
XOR result	0011	
fk(xor result, R)	0011	0001
fk result	00110001	
SW	00010011	

SECOND Fk

L	0001	
R	0011	
SK	01011111	

E/P input	0011	
E/P result	10010110	
XOR input	10010110,	01011111
XOR result	11001001	
s0 input	1100	
s0 array	1032	
	3210	
	0213	
	3132	
s0row result	dec(2)	
s0column result	dec(2)	
s0bin result	01	
s1 input	1001	
s1 array	0123	
	2013	
	3010	
	2103	
s1row result	dec(3)	
s1column result	dec(0)	
s1bin result	10	
s0+s1 result	0110	
p4 input	0110	
p4 result	1010	
XOR (L, p4 result)	0001	1010
XOR result	1011	
fk(xor result, R)	1011	0011
fk result	10110011	
ip-1 input	10110011	
ip-1 result	11101010	
first 4 bits	1110	
second 4 bits	1010	
plaintext	OK	

0 0000 A	1 0001 B	2 0010 C	3 0011 D	4 0100 E	5 0101 F	6 0110 G
7 0111 H	8 1000 I	9 1001 J	10 1010 K	11 1011 L	12 1100 M	13 1101 N
14 1110 O	15 1111 P					

0	1	2	3	4	5	6
0000	0001	0010	0011	0100	0101	0110
A	B	C	D	E	F	G
7	8	9	10	11	12	13

0111	1000	1001	1010	1011	1100	1101
H	I	J	K	L	M	N
14	15					
1110	1111					
O	P					