Problem 3

Consider the following SPN:

- the subblock length is $n = 4$,
- a plaintext consists of $m = 8$ subblocks,
- the key length is $s = 32$,
- the number of rounds is $r = 3$,
- the S-Box is defined as follows:

0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
1111	0100	1101	0110	0000	1100	1011	1110	0111	0010	1010	0101	1001	0011	1000	0001

- the permutation is defined as follows:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
7	4	3	2	1	11	14	0	13	12	15	5	9	8	6	10	23	19	31	17	26	30	22	16	29	25	20	28	27	24	21	18

- the round key is $K(k, i) = k$, for $i \leq 3$.

The approximation chart for the S-Box is given as follows:

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	$-\frac{1}{8}$	0	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{8}$	0	$-\frac{1}{4}$	$\frac{1}{8}$	0	$\frac{1}{8}$	$-\frac{1}{8}$	0	$\frac{1}{8}$	0
0010	0	0	0	$\frac{1}{4}$	0	0	0	$-\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$
0011	0	$-\frac{1}{8}$	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	$\frac{3}{8}$	0	$\frac{1}{8}$	0	$\frac{1}{8}$	0	0	$\frac{1}{8}$	0	$\frac{1}{8}$
0100	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	0
0101	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	$-\frac{1}{8}$	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{4}$	0	$\frac{1}{8}$	$\frac{1}{4}$	$-\frac{1}{8}$	$\frac{1}{8}$	0
0110	0	0	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	0	0	$-\frac{1}{8}$	$-\frac{3}{8}$
0111	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{4}$	$-\frac{1}{8}$	0	0	$\frac{1}{8}$	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{4}$	$-\frac{1}{8}$	0	0	$\frac{1}{8}$
1000	0	$\frac{1}{8}$	0	$\frac{1}{8}$	$-\frac{1}{4}$	$-\frac{1}{8}$	0	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{8}$	0	$\frac{1}{8}$	0	$\frac{1}{8}$	0
1001	0	$-\frac{1}{4}$	0	0	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{4}$	0	0	0
1010	0	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{8}$	0	$\frac{1}{8}$	0	$-\frac{1}{8}$	0	$-\frac{1}{8}$	$\frac{1}{4}$	$-\frac{1}{8}$	0	$-\frac{1}{8}$	0	$\frac{1}{8}$
1011	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	0	0	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$
1100	0	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	0	0	$-\frac{3}{8}$	$-\frac{1}{8}$	0
1101	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	?	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{4}$	0
1110	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	$-\frac{1}{8}$	0	$\frac{1}{4}$	$\frac{1}{8}$	$-\frac{1}{8}$	0	$-\frac{1}{4}$	$\frac{1}{8}$
1111	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	0	$-\frac{1}{4}$	$-\frac{1}{8}$	$\frac{1}{8}$	0	$-\frac{1}{4}$	0	0	$\frac{1}{8}$	$\frac{1}{8}$

In this table, the numbers reflect the biases as follows: For instance the entry in row 0101 *and column* 1011 *is* $2(\Pr[x[1,3] \oplus S(x)[0,2,3] = 0] - \frac{1}{2}) = 2\epsilon$.

a) Compute the missing value in the so called approximation chart that states the biases in the S-Box for all subsets S_0 and S_1.

b) Determine the linear relation between the plaintext bits, key bits and $S(x)[2]$. Hint: Start with $x[2] \oplus S(x)[2,3] = 0$ for the S-Box.

c) Given are a plaintext-cyphertext pair and a potential key:

x	0111	0110	0101	0100	0000	1001	1011	1100
y	1010	1010	0001	0100	0100	1111	1011	1000
k	0100	1001	0100	1010	0101	0011	0101	1001

Check whether your equation from b) holds for those values.