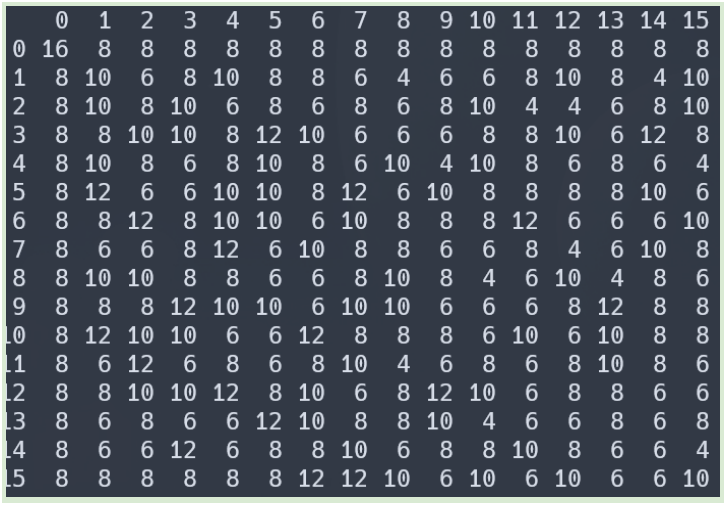
1. Write a C/C++ program to compute the linear approximation table for this S-box

   In the picture below, here is the generated output of the linear approximation table.



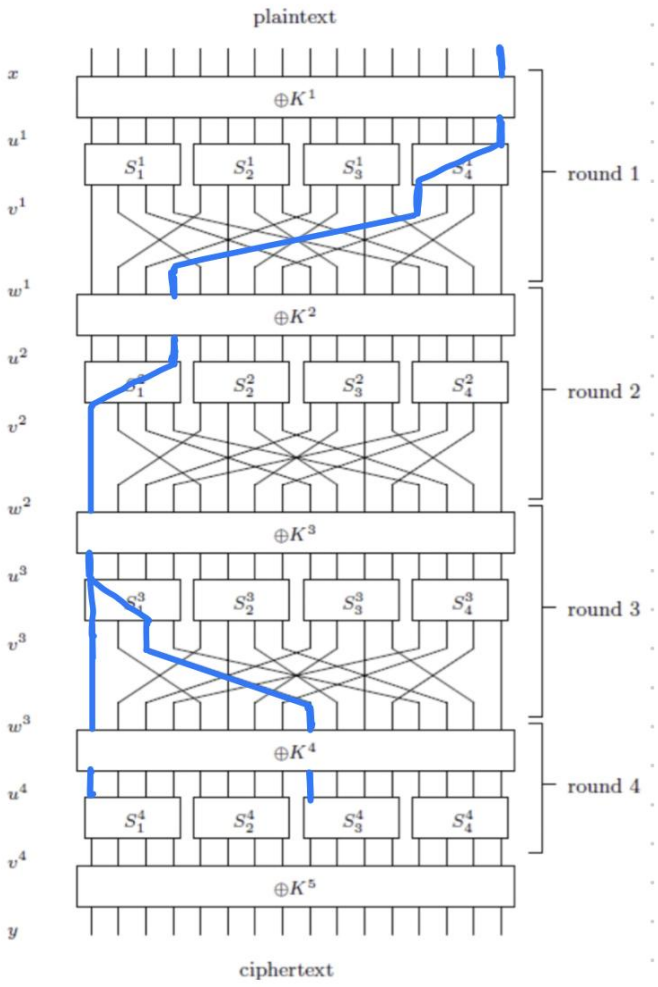
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	10	6	8	10	8	8	6	4	6	6	8	10	8	4	10
2	8	10	8	10	6	8	6	8	6	8	10	4	4	6	8	10
3	8	8	10	10	8	12	10	6	6	6	8	8	10	6	12	8
4	8	10	8	6	8	10	8	6	10	4	10	8	6	8	6	4
5	8	12	6	6	10	10	8	12	6	10	8	8	8	8	10	6
6	8	8	12	8	10	10	6	10	8	8	8	12	6	6	6	10
7	8	6	6	8	12	6	10	8	8	6	6	8	4	6	10	8
8	8	10	10	8	8	6	6	8	10	8	4	6	10	4	8	6
9	8	8	8	12	10	10	6	10	10	6	6	6	8	12	8	8
10	8	12	10	10	6	6	12	8	8	8	6	10	6	10	8	8
11	8	6	12	6	8	6	8	10	4	6	8	6	8	10	8	6
12	8	8	10	10	12	8	10	6	8	12	10	6	8	8	6	6
13	8	6	8	6	6	12	10	8	8	10	4	6	6	8	6	8
14	8	6	6	12	6	8	8	10	6	8	8	10	8	6	6	4
15	8	8	8	8	8	8	12	12	10	6	10	6	10	6	6	10

   The C++ code will be provided as a different file.

2. Find a linear approximation using three active S-boxes and use the piling-up lemma (you need to research about it) to estimate the bias of the random variable

$$X_{16} \oplus U_1^4 \oplus U_4^9$$

   In order to find the linear approximation using three active S-Boxes, we first have to indicate what the Active S boxes are. Given the random variables, we can find the corresponding lines within the given SPN. The blue lines drawn in the figure are the paths that show the active S-Boxes.



So the 3 active S-Boxes with the bias according to the LAT are:

S^1_4 = (The random Variable $T_1 = U^1_6 \oplus V^1_{13}$ has bias -1/4)

S^2_1 = (The random Variable $T_2 = U^2_4 \oplus V^2_1$ has bias -1/4)

S^3_1 = (The random Variable $T_3 = U^3_1 \oplus V^3_1 \oplus V^3_3$ has bias -1/4)

The piling Lemma is defined as $2^{n-1} \prod \varepsilon_i = 2^{3-1} * -¼ * -¼ * -¼ = -1/16$

3. Implement a linear attack to find the eight sub-key bits in the last round (corresponding to the linear approximation in (b)). The plaintext-ciphertext pairs (encrypted with the same key) are in the le pairs (on each line in pairs the first is the plaintext and the second is the ciphertext; in decimal - convert to binary). You have to write a C/C++ program which reads the pairs from pairs le and outputs the biases for all candidate sub-keys. You pick then the right eight sub-key bits.