



Problem 3. «Steganography and codes»

Sam and Betty use public channel for their private communication. They want that nobody knows about the fact of their dialog.

They agreed that Sam can send to Betty one of the following sixteen messages:

- 0 — «Everything is OK», 1 — «I miss you», 2 — «I miss you too much!»,
- 3 — «Call me, please», 4 — «Where are you?», 5 — «YES!», 6 — «NO!»,
- 7 — «I said NO!», 8 — «I don't know», 9 — «I'm working now»,
- 10 — «I'm walking now», 11 — «I'm not available now», 12 — «I will come soon»,
- 13 — «I'm studying cryptography and think that it is a very great thing!»,
- 14 — «Go to the NSUCRYPTO next year with me!»,
- 15 — «Bye, bye! See you tomorrow».

Sam takes any picture in RGB format, changes the first pixel of it in some way and publishes the modified picture on his web-cite. Betty downloads the picture, analyzes it and takes out the message for her.

What does the Sam do with the picture? He should change it in such a way that nobody can visually fix the changing.

One pixel of a picture in format RGB is represented with 24 bits:

- 8 bits for brightness of red color (r_1, \dots, r_8) ,
- 8 bits for brightness of green color (g_1, \dots, g_8) ,
- and 8 bits for brightness of blue color (b_1, \dots, b_8) .

It is not possible for Sam to change bits r , g and b with numbers $1, \dots, 5$ since it makes a changing to be visual. If Sam changes one of bits r_6, r_7, g_6, g_7 and b_6 , let us say that it costs 2 coins, while changing of one bit between r_8, g_8, b_7 and b_8 costs 1 coin.

Propose a method of coding a message (through given 16 types) in one pixel such it costs not more than 2 coins (in this case the changing of the picture is still not visual). Propose also the method for Betty how to extract secret messages. It is important that she has no access to the original picture.

