Zadanie 3

Liniowym branch number dla przekształcenia F nazywamy:

$$B_l(F) = \min_{\alpha \neq 0, \beta, LAT(\alpha,\beta) \neq 0} \quad w(\alpha) \oplus w(\beta),$$

gdzie $w(x)$ to waga Hamminga, a $\alpha \in \{0,1\}^n$ i $\beta \in \{0,1\}^n$ to maski liniowe odpowiednio dla ciągu wejściowego $X_0X_1 \ldots X_{n-1}$ i wyjściowego $Y_0Y_1 \ldots Y_{n-1}$.

Mrożon chce uratować świat przed Probabilistami. Aby mu się to udało, musi wybrać szyfr, którego przekształcenie F ma większe liniowe branch number.

Przekształcenie F_i szyfru Icicle ma LAT-profil następującej postaci:

	0	1	2	3	4	5	6	7
0	4	0	0	0	0	0	0	0
1	0	2	0	-2	0	2	0	2
2	0	0	-2	-2	0	0	2	-2
3	0	2	-2	0	0	-2	-2	0
4	0	2	0	2	-2	0	2	0
5	0	0	0	0	2	-2	2	2
6	0	-2	-2	0	-2	0	0	2
7	0	0	2	-2	-2	-2	0	0

Natomiast przekształcenie $F_f : Z_2^3 \to Z_2^3$ szyfru Frozone działa w następujący sposób:

$$F_f(0) = 2, \quad F_f(1) = 1,$$
$$F_f(2) = 5, \quad F_f(3) = 6,$$
$$F_f(4) = 7, \quad F_f(5) = 4,$$
$$F_f(6) = 0, \quad F_f(7) = 3.$$

Czy pomożesz Mrożonowi uratować świat?

Aby to zrobić wpisz flagę w postaci nazwaszyfru_branchnumber, gdzie obie wartości dotyczą szyfru z większym liniowym branch number, np. jeśli $B_l(F_i) = 4$ i $B_l(F_f) = 1$, to flagą będzie Icicle_4.