



Dvigubas kodavimas

UŽDUOTIS

Modernus kodavimo standartas (MKS) pateikė naują algoritmą. Algoritmas dirba su trimis *blokais*, kiekvienas kurių sudarytas iš 128 bitų. Duotas blokas p (pradinis tekstas) ir raktinis blokas k . MKS kodavimo funkcija E grąžina užkoduotą bloką c :

$$c = E(p, k).$$

Funkcijai E atvirkščia yra dekodavimo funkcija D :

$$D(E(p, k), k) = p, \quad E(D(c, k), k) = c.$$

Naudojant *dvigubą MKS kodavimą*, paėliui naudojami du nepriklausomi raktiniai blokai k_1 ir k_2 . Pirmiau taikomas raktas k_1 , paskui k_2 :

$$c_2 = E(E(p, k_1), k_2).$$

Taip pat duotas sveikasis skaičius s , kuris nusako raktinių blokų struktūrą: reikšminiai yra tik kairiausi $4*s$ bitų, tuo tarpu likusieji (dešiniai 128– $4*s$) bitai yra lygūs 0. Skaičius s yra tas pats abiem raktams.

Jums duotas pradinis tekstas p , jį atitinkantis dvigubai užkoduotas tekstas c_2 , bei raktinių blokų struktūra, kurią nusako sveikasis skaičius s . Raskite kodavimo raktų (t.y. blokų) porą, kuri buvo panaudota pranešimui užkoduoti.

Kodavimo ir dekodavimo algoritmai pateikti bibliotekoje.

Jūs turite pateikti tik surastus raktinius blokus. Programos pateikti nereikia.

PRADINIAI DUOMENYS

Dešimt pradinių duomenų rinkinių duoti tekstinėse bylose, pavadintose vardais nuo `double1.in` iki `double10.in`. Kiekvieną bylą sudaro trys eilutės. Pirmoje eilutėje įrašytas sveikasis skaičius s , antroje – pradinis blokas p , o trečioje – dvigubai užkoduotas blokas c_2 . Abu blokai pateikti 32 šešioliktainių skaitmenų ('0'..'9', 'A'..'F') eilutėmis. Bibliotekoje numatyta galimybė eilutes paversti blokais. Pradiniai duomenys tokie, kad sprendinys egzistuoja.

REZULTATAI

Jums reikia pateikti dešimt rezultatų bylų, atitinkančių pradines bylas. Kiekvieną rezultatų bylą turi sudaryti trys eilutės. Pirmoje eilutėje turi būti įrašytas tekstas:

```
#FILE double I
```

