



Slaptas pranešimas

Pranešimą sudaro 0 ir 1 skaitmenų seka. Pranešimas yra šifruojamas, panaudojant slaptą raktą. Šifro raktas yra fiksuoto ilgio skaitmenų 0 ir 1 seka.

Šifruojama taip: pranešimas nuosekliai, pradedant nuo pradžios, suskaidomas į blokus, kurių ilgiai lygūs rakto ilgiui; paskutinis blokas gali turėti ir mažiau skaitmenų negu raktas. Kiekvienas blokas šifruojamas, keičiant kiekvieną jo skaitmenį atsižvelgiant į atitinkamą rakto skaitmenį pagal tokią taisyklę:

Pranešimo skaitmuo	Rakto skaitmuo	Užšifruoto pranešimo skaitmuo
0	0	0
0	1	1
1	0	1
1	1	0

Šifravimo taisyklę galima užrašyti tokia formule:

$$\text{Užšifruoto_pranešimo_skaitmuo} = (\text{Pranešimo_skaitmuo} + \text{Rakto_skaitmuo}) \bmod 2.$$

Šifravimo pavyzdys: pranešimas 0 1 1 0 1 0 0 1, raktas 1 1 0; tada,

pranešimas, suskaidytas į blokus: 0 1 1 0 1 0 0 1

pranešimas, suskaidytas į blokus: 1 1 0 1 1 0 1 1

užšifruotas pranešimas: 1 0 1 1 0 0 1 0

Nesunku matyti, kad turint užšifruotą pranešimą ir šifravimo raktą, pranešimas gali būti iššifruotas panaudojant analogišką procedūrą.

Buvo gautas užšifruotas pranešimas. Šifro raktas nėra žinomas, tačiau spėjama, kad neužšifruotame pranešime turi būti sutinkama tam tikra skaitmenų seka. Padėkite surasti šifro raktą ir iššifruoti pranešimą.

Užduotis. Duotas užšifruotas pranešimas ir seka – spėjama pradinio (neužšifruoto) pranešimo dalis. Parašykite programą, kuri surastų trumpiausią tinkamą šifravimo raktą ir nurodytą, kurioje iššifruoto pranešimo vietoje yra spėjama seka.

Raktas tinkamas, jei spėjama seka yra šiuo raktu iššifruoto pranešimo dalis ir rakto ilgis neviršija $N \div 2$ (čia N – spėjamos sekos ilgis).

Jei yra keli sprendiniai (keli trumpiausi raktai arba spėjama seka sutinkama keliose pranešimo vietose), reikia pateikti bet kurį vieną.

Pradiniai duomenys. Pirmoje eilutėje įrašytas spėjamos sekos (t.y. spėjamos pranešimo dalies) ilgis N . Antroje eilutėje įrašyti spėjamos sekos skaitmenys atskirti tarpais. Trečioje eilutėje įrašytas užšifruoto pranešimo ilgis P , o ketvirtojoje – užšifruoto pranešimo skaitmenys, atskirti tarpais.

Rezultatai. Jei nerastas tinkamas šifro raktas, rezultatas turi būti lygus 0, įrašytam pirmoje eilutėje.



Priešingu atveju pirmoje eilutėje turi būti įrašytas trumpiausio tinkamo šifro rakto ilgis, o antroje eilutėje – rakto skaitmenys, atskirti tarpais.

Trečioje eilutėje reikia įrašyti poziciją (jos numeruojamos nuo 1), ties kuria iššifruotame pranešime prasideda spėjama seka. Ketvirtoje eilutėje reikia įrašyti pranešimo ilgį, o penktoje – iššifruoto pranešimo skaitmenis atskirtus tarpais.

Pavyzdžiai.

Pradiniai duomenys	Rezultatai
2 0 0 4 0 1 1 0	1 1 2 4 1 0 0 1

Pradiniai duomenys	Rezultatai	Paiškinimas
5 1 1 0 0 1 12 1 1 0 1 1 0 0 0 1 1 1 1	2 1 0 3 12 0 1 1 1 0 0 1 0 0 1 0 1	Spėjamos sekos ilgis 5. Pati seka: 1 1 0 0 1 Pranešimo ilgis 12. Užšifruotas pranešimas: 1 1 0 1 1 0 0 0 1 1 1 1.

Pradiniai duomenys	Rezultatai	Paiškinimas
5 1 1 0 0 1 12 1 1 0 1 1 0 0 0 1 1 1 1	2 1 0 3 12 0 1 1 1 0 0 1 0 0 1 0 1	Trumpiausio tinkamo šifro rakto ilgis 2. Rastas šifro raktas: 1 0. Spėjama seka (1 1 0 0 1), sutinkama pranešime nuo 3 pozicijos. Iššifruotas pranešimas (ilgis 12): 0 1 1 1 0 0 1 0 0 1 0 1.

Ribojimai. $2 \leq P \leq 20\,000$;

$2 \leq N \leq 120$;

$N \leq P$.