

# Rejestr

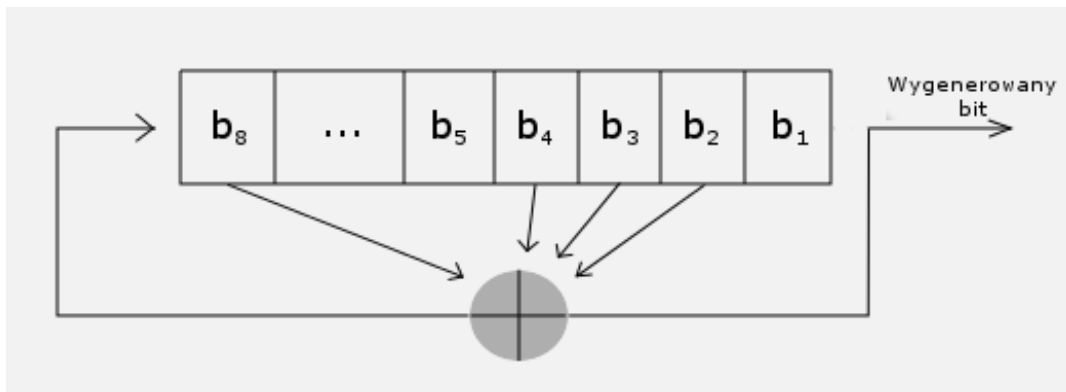
Do budowy pseudolosowych generatorów strumieniowych często wykorzystuje się rejestry. Generatory takie mają szerokie zastosowanie w kryptografii. Im bardziej wyrafinowany system generujący bity, tym trudniej jest go złamać. Nasz generator jest oparty na rejestrze przesuwającym ze sprzężeniem zwrotnym. Działanie jego jest bardzo proste. Ustalamy według pewnego schematu (o tym w dalszej części zadania) komórki rejestru, z których sumowane są bity modulo 2. Wynik jest wygenerowanym bitem, który także jest wstawiany na koniec rejestru, natomiast pozostałe są przesuwane o jeden bit w prawo.

Aby uzyskać maksymalny cykl takiego generatora należy oprzeć go o wielomian pierwotny modulo 2 (autor zadania zadbał o to, żeby tylko takie pojawiły się na wejściu). Wielomian, który został przedstawiony w zadaniu ma postać:

$$x^8+x^4+x^3+x^2+1$$

Rejestr ma zawsze długość stopnia wielomianu. W tym przypadku jest to 8 bitów. Zaczepy bitów, które będziemy dodawać modulo 2 ustawiamy odpowiednio na 8, 4, 3 oraz 2 miejscu (wyraz wolny nie bierze udziału).

Rysunek przedstawia generator dla wielomianu podanego w przykładzie:



Zadanie polega na odszyfrowaniu wiadomości zaszyfrowanej tym generatorem.

## Szyfrowanie

Najpierw ustawiamy ziarno - wartości początkowe bitów zawartych w poszczególnych komórkach rejestru. Następnie uruchamiamy generator pewną ilość razy. Następnie generujemy partie po osiem bitów i xorujemy je z kodem ASCII danej litery. W ten sposób powstaje szyfrogram w postaci sekwencji bitów - jedna litera = 8 bitów. Twoje zadanie polega na odszyfrowaniu wiadomości i przedstawieniu jej w postaci znakowej.

## Wejście

W pierwszym wierszu jedna liczba  $n$  określająca stopień wielomianu pierwotnego ( $n < 10000$ ).

W drugim wierszu  $n+1$  współczynników tego wielomianu począwszy od tego, który stoi przy najwyższej potędze (współczynniki należą do zbioru  $\{0, 1\}$ ).

Następnie ustawienie ziarna -  $n$  bitów rejestru.

W czwartym wierszu jedna liczba  $u$  określająca po ilu uruchomieniach generatora, bity będą brane pod uwagę.

W ostatnim wierszu szyfrogram o długości  $8 \cdot s$  ( $1 \leq s \leq 500000$ ).

Dodatkowo  $n \cdot s < 10^8$  oraz  $n \cdot u < 10^8$

## Wyjście

Oryginalna wiadomość.

## Przykład

**Wejście:**

8

1 0 0 0 1 1 1 0 1

1 1 1 0 0 1 0 1

2

0101001000010101100000101011011011010101

**Wyjście:**

haker