Szyfrowanie z kluczem prywatnym oraz publicznym

Klucz prywatny

Określmy długość klucza np. 5. Generujemy superrosnący ciąg złożony z pięciu elementów np. 2 3 6 13 27 (ciąg superrosnący to taki, w którym i-ty wyraz jest większy niż suma wszystkich wyrazów jego poprzedzających).

Klucz publiczny

Określamy liczbę **n**, która jest większa od sumy wszystkich liczb ciągu superrosnącego np. 53 oraz określamy mnożnik **m**, który musi być względnie pierwszy ze wszystkimi liczbami superrosnącego ciągu, np. 17. Klucz publiczny tworzymy według schematu:

a_i*m mod n, gdzie a_i to kolejne wyrazy superrosnącego ciągu:

2*17 **mod** 53 = 34
3*17 **mod** 53 = 51
6*17 **mod** 53 = 49
13*17 **mod** 53 = 9
27*17 **mod** 53 = 35

A więc klucz publiczny ma postać: 34, 51, 49, 9, 35.

Szyfrowanie

Wiadomość do zaszyfrowania zapisujemy w postaci binarnej, następnie dzielimy ją na sekwencje o długości klucza, w naszym przypadku sekwencja jest długości pięciu bitów. Następnie i-ty bit przemnażamy przez i-ty element klucza publicznego:

Wiadomość: 10001 10011
Szyforgram: (1*34 + 1*35, 1*34 + 1*9 + 1*35) = (69, 78)

Deszyfrowanie

Odbiorca wiadomości posiada klucz prywatny oraz liczby **n** i **m**. W celu odszyfrowania wiadomości odbiorca musi najpierw określić $\mathbf{n}(\mathbf{n}^{-1})\equiv 1$ **mod m**. Mnożąc każdą liczbę szyfrogramu przez $\mathbf{n}^{-1}$ **mod m**, otrzymuje wartości wiadomości szyfrowanej (tekstu jawnego).

Zadanie

Dla danego klucza pywatnego, liczb **n** i **m** utwórz klucz publiczny i zaszyfruj wiadomość.

Wejście

W pierwszym wierszu jedna liczba **d** określająca długość klucza prywatnego (nie większa niż 20).
W drugim wierszu **d** liczb określających klucz prywatny.

W trzecim wierszu liczby **n** i **m**.
W ostatnim wierszu wiadomość w postaci binarnej do zaszyfrowania (nie dłuższa niż 1000 bitów). Liczba bitów jest liczbą podzielną przez **d**.
Wszystkie liczby są nie większe niż 10^7 i spełniają założenia opisanego wyżej szyfrowania.

Wyjście

Ciąg liczb będący szyfrogramem

Przykład

Wejście:
5
2 3 6 13 27
53 17
1000110011

Wyjście:
69 78