Vigenère Codering

De Vigenère codering is in de cryptografie één van de klassieke methodes om tekst te versleutelen. De methode werd oorspronkelijk beschreven door Giovanni Batista Bellaso in zijn boek La cifra del Sig uit 1553, maar raakte pas in de 19^e eeuw algemeen bekend door Blaise de Vigenère, waardoor het zijn naam kreeg.

Opgave

Om een tekst te versleuten kiest men eerst een geheim sleutelwoord, bijvoorbeeld `VPW`. Dit sleutelwoord, dat geen spaties bevat, wordt herhaald totdat een string verkregen wordt met dezelfde lengte als de oorspronkelijke tekst die moet gecodeerd worden (de herhaling wordt hiertoe achteraan afgebroken). Dit herhaalde sleutelwoord schrijft men dan onder de oorspronkelijke tekst.

```
VLAAMSE PROGRAMMEERWEDSTRIJD
++++++++++++++++++++++++++++
VPWVPWVPWVPWVPWVPWVPWVPWVPWV
============================
QAXWBO PLMDCMQIHUAMLAZHPMYFZ
```

Vervolgens telt men de corresponderende letters uit de originele tekst en het sleutelwoord bij elkaar op. Bij deze optelling worden de letters A tot Z beschouwd als de getallen 1 tot 26, een spatie krijgt de waarde 0. De optelling wordt uitgevoerd modulo 27 (het aantal letters uit het alfabet plus de spatie). In het bovenstaande voorbeeld krijgen we dus $\texttt{V} + \texttt{V} = (22 + 22) \mod 27 = 17 = \texttt{Q}$.

Het ontcijferen van een boodschap gebeurt analoog. Men trekt gewoon de waarde van de overeenkomstige codeletter af van de gecodeerde letter. In het voorbeeld hierboven krijgen we dan $\texttt{Z} - \texttt{V} = (26 - 22) \mod 27 = 4 = \texttt{D}$.

Het is de bedoeling een programma te schrijven dat teksten kan coderen en decoderen volgens een gegeven sleutelwoord.

Invoer

De invoer bestaat uit een aantal te coderen boodschappen met bijhorende sleutel. Er worden ook een aantal te decoderen boodschappen gegeven, opnieuw met bijhorende sleutel. De boodschappen en codewoorden worden in hoofdletters gegeven en bevatten geen leestekens. De eerste lijn bevat een

getal n dat aangeeft hoeveel te versleutelen boodschappen er worden gegeven. Daarop volgen n lijnen die telkens een sleutelwoord en een boodschap bevatten. Het eerste woord op elke lijn is het sleutelwoord, de rest van de lijn omvat de boodschap. Na deze n lijnen komt een lijn die een getal m bevat dat aangeeft hoeveel boodschappen moeten worden gedecodeerd. De m daaropvolgende lijnen bevatten telkens een codewoord en een verleutelde boodschap. Het eerste woord is het codewoord, de rest van de lijn is de versleutelde boodschap.

Uitvoer

De uitvoer bestaat uit $(n + m)$ lijnen. De eerste n lijnen bevatten de gecodeerde boodschappen, de m daaropvolgende lijnen bevatten de gedecodeerde boodschappen, beide in de volgorde waarin ze aan de invoer verschenen.

Voorbeeld

In dit voorbeeld hebben we 2 testgevallen waarin gevraagd wordt de gecodeerde tekst te bepalen en één testgeval waarin de gedecodeerde tekst wordt gevraagd.

Invoer

```
2
VPW VLAAMSE PROGRAMMEERWEDSTRIJD
ARISTOTELES DANKBAARHEID VEROUDERT SNEL
1
CODE GXXELGDJHBDLUCSYCVIMHXQ
```

Uitvoer

```
QAXWBO PLMDCMQIHUAMLAZHPMYFZ
ESWCVPUWTJAERDXKCNIQWLAJWXE
DIT IS EEN GROOT GEHEIM
```