Vigenère cipher

In cryptography, the Vigenère cipher is one of the classic methods to encode and decode text messages. The Vigenère cipher has been reinvented many times. The method was originally described by Giovan Battista Bellaso in his 1553 book *La cifra del sig*. However, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the Vigenère cipher.

To encode a given text message, a secret keyword is chosen, for example `ZODIAK`. The keyword can only contain uppercase letters (no spaces), and is repeated until one obtains a string that has the same length as the original text that needs to be encoded (to achieve this, the repetition is stripped at the end). The repeated keyword is then written below the original text.

```
   plaintext : THIS IS EXTREMELY SECRET!
             ++++++++++++++++++++++++
     keyword : ZODIAKZODIAKZODIAKZODIAKZ
             ========================
  ciphertext : SVLA SR HFTBDAHTY RSFZED!
```

Each letter in the original text is than added to the corresponding letter of the keyword. In this addition, the letters `A` to `Z` are considered to have integer values 0 to 25. The addition is done modulo 26 (corresponding to the number of letters in the alphabet). The Vigenère cipher can thus be written as $$C_i = O_i + K_i\ (\mathrm{mod}\ 26)\,,$$ where C_i represents the i-th letter of the ciphertext, O_i represents the i-the letter of the original text and K_i represents the i-th letter of the (repeated) keyword. At the first position in the above example we thus get $\mathrm{T} + \mathrm{Z} = 19 + 25\ (\mathrm{mod}\ 26) = 18 = \mathrm{S}$.

A similar procedure is use to decode an encoded message, where a letter of the keyword is subtracted from the corresponding letter in the encoded message. The decoding procedure of the Vigenère cipher can thus be written as $$O_i = C_i - K_i\ (\mathrm{mod}\ 26)\,.$$

Assignment

- Write a function `encode` that encrypts a given text message t according to the Vigenère cipher with given keyword s that only contains uppercase letters. The text message t and the keyword s must be passed as arguments to the function. The function must return the encrypted text message. In doing so, only the uppercase letters in the given text message must be encoded. Other characters (lowercase letters, spaces, digits, punctionation marks, …) must remain unchanged in the encrypted message.
- Write a function `decode` as the dual function of the function `encode`. This function must therefore decrypt a given text message t according to the Vigenère cipher with given keyword s that only contains uppercase letters. The encrypted text message t and the keyword s must be passed as arguments to the function. The function must return the decrypted text message. In doing so, only the uppercase letters in the given text message must be decoded. Other characters (lowercase letters, spaces, digits, punctionation marks, …) must remain unchanged in the decrypted message.

Example

```
>>> encode('NOBODY EXPECTS THE SPANISH INQUISITION!', 'CIRCUS')
'PWSQXQ MORYUVA VBW AGCHAUP KHIWQJKNAQV!'

>>> decode('PWSQXQ MORYUVA VBW AGCHAUP KHIWQJKNAQV!', 'CIRCUS')
'NOBODY EXPECTS THE SPANISH INQUISITION!'

>>> encode('OH SHUT UP! AND GO AND CHANGE YOUR ARMOUR!', 'ARTHUR')
'OY ZBLT NW! AEW AF RGK THRGNY YFNY RRDHBL!'

>>> decode('OY ZBLT NW! AEW AF RGK THRGNY YFNY RRDHBL!', 'ARTHUR')
'OH SHUT UP! AND GO AND CHANGE YOUR ARMOUR!'
```

De Vigenèrecodering is in de cryptografie één van de klassieke methoden 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 19e eeuw algemeen bekend door Blaise de Vigenère, waardoor het zijn naam kreeg.

Om een tekst te versleuten kiest men eerst een geheim sleutelwoord, bijvoorbeeld ZODIAK. 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.

```
originele tekst : DIT IS EXTREEM GEHEIM!
                  ++++++++++++++++++++++
  sleutelwoord : ZODIAKZODIAKZODIAKZODI
                  ======================
versleutelde tekst : CWW IC SABRODA OERDWP!
```

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 0 tot 25. De optelling wordt uitgevoerd modulo 26 (het aantal letters in het alfabet). De Vigenèrecodering kan dus worden geschreven als $$V_i = O_i + S_i\ (\mathrm{mod}\ 26)\,,$$ waarbij V_i de i-de letter uit de versleutelde tekst voorstelt, O_i de i-de letter uit de originele tekst en S_i de i-de letter uit het sleutelwoord. Voor de eerste letter uit het bovenstaande voorbeeld krijgen we dus $\mathrm{D} + \mathrm{Z} = 3 + 25\ (\mathrm{mod}\ 26) = 2 = \mathrm{C}$.

Om te ontcijferen gebruikt men een gelijkaardige procedure, waarbij een letter van het sleutelwoord van de corresponderende letter uit het gecodeerde bericht wordt afgetrokken. De Vigenèrecodering kan dus worden geschreven als $$O_i = V_i - S_i\ (\mathrm{mod}\ 26)\,.$$

Opgave

- Schrijf een functie codeer die een gegeven tekst t versleutelt volgens de Vigenèrecodering op basis van een gegeven sleutel s die enkel uit hoofdletters bestaat. De originele tekst t en de sleutel s moeten als argument aan de functie doorgegeven worden. De functie moet de versleutelde tekst als resultaat teruggegeven. Hierbij moeten enkel de hoofdletters uit de originele tekst versleuteld worden. Alle overige karakters (kleine letters, spaties, cijfers, leestekens, …) blijven ongewijzigd in de gecodeerde tekst.
- Schrijf een functie decodeer als duale functie van de functie codeer. Deze functie moet dus een gegeven tekst t ontcijferen volgens de Vigenèredecodering op basis van een gegeven sleutel s die enkel uit hoofdletters bestaat. De versleutelde tekst t en de

sleutel s moeten als argument aan de functie doorgegeven worden. De functie moet de ontcijferde tekst als resultaat teruggegeven. Hierbij moeten enkel de hoofdletters uit de versleutelde tekst ontcijferd worden. Alle overige karakters (kleine letters, spaties, cijfers, leestekens, …) blijven ongewijzigd in de ontcijferde tekst.

Voorbeeld

```
>>> codeer('NOBODY EXPECTS THE SPANISH INQUISITION!', 'CIRCUS')
'PWSQXQ MORYUVA VBW AGCHAUP KHIWQJKNAQV!'

>>> decodeer('PWSQXQ MORYUVA VBW AGCHAUP KHIWQJKNAQV!', 'CIRCUS')
'NOBODY EXPECTS THE SPANISH INQUISITION!'

>>> codeer('OH SHUT UP! AND GO AND CHANGE YOUR ARMOUR!', 'ARTHUR')
'OY ZBLT NW! AEW AF RGK THRGNY YFNY RRDHBL!'

>>> decodeer('OY ZBLT NW! AEW AF RGK THRGNY YFNY RRDHBL!', 'ARTHUR')
'OH SHUT UP! AND GO AND CHANGE YOUR ARMOUR!'
```