Zadanie Szyfr Vigenère'a – LOGIA 19 SP (2018/19), etap 2

Treść zadania

Ania do szyfrowania wiadomości wykorzystuje tabelę liter (rysunek obok) oraz klucz. Każdej literze tekstu jawnego przyporządkowuje literę z tabeli znajdującą się na przecięciu wiersza wyznaczanego przez tę literę i kolumny odpowiadającej kolejnej literze klucza. Jeżeli długość klucza jest mniejsza niż długość tekstu szyfrowanego, to powiela klucz.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Przykład dla klucza **LOGIA** i tekstu szyfrowanego **OLAMAKOTA**:

tekst jawny: `OLAMAKOTA`

klucz: `LOGIALOGI`

szyfrogram: `ZZGUAVCZI`

Zdefiniuj dwuparametrową funkcję **deszyfr**, której parametrami są dwa słowa o długości od **1** do **1000** złożone z wielkich liter alfabetu łacińskiego, odpowiednio szyfrogram i klucz. Wynikiem jest słowo będące odszyfrowanym tekstem jawnym.

Przykłady:

Wynikiem **deszyfr("ZZGUAVCZI", "LOGIA")** jest **"OLAMAKOTA"**.

Wynikiem **deszyfr("CGSMURRBO", "KRET")** jest **" SPOTKANIE "**.

Omówienie rozwiązania

Podczas analizy działania szyfru Vigenère'a opartego na tablicy z treści zadania należy zauważyć, że każdy z wierszy odpowiada szyfrowi Cezara, przy czym w pierwszym wierszu przesunięcie wynosi 0, w drugim 1 itd. Szyfr Cezara jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest inną, oddaloną od niej o stałą liczbę pozycji w alfabecie. Zakładamy, że alfabet „zawija się" i za literką Z następuje znów litera A.

Do szyfrowania można użyć kodu ASCII, który przyporządkowuje każdej literze liczbę, na przykład kod ASCII litery **A** to **65**, litery **K** to **75**, a litery **Z** to **90**.

OEiiZK
Ośrodek Edukacji Informatycznej
i Zastosowań Komputerów w Warszawie

Odszyfrowanie tekstu to tak naprawdę ponowne zaszyfrowanie z kluczem będącym jego dopełnieniem do 26 (liczba liter alfabetu łacińskiego.). Jeśli tekst jawny zaszyfrowano z kluczem 12, to odszyfrowanie polega na zaszyfrowaniu kryptogramu kluczem 26 – 12 = 14, co oznacza, że trzeba przesunąć się do przodu o 14 liter.

Rozwiązanie w języku Python

Aby otrzymać kod ASCII danego znaku, należy wykorzystać funkcję **ord(znak)** – na przykład wynikiem **ord("K")** będzie **75**. Odwrotna funkcja to **chr(kod)**. Pozwala ona otrzymać znak odpowiadający danemu kodowi ASCII – na przykład wynikiem **chr(90)** będzie **Z**.

Aby zaszyfrować jeden znak danym kluczem należy zamienić literę na kod ASCII, odjąć od niej kod ASCII litery A, a następnie dodać klucz. Kolejne działanie to obliczenie reszty z dzielenia wyniku przez 26, dodanie kodu ASCII litery A i zamiana całości na literę.

Funkcja **ktora(litera)** daje w wyniku numer litery od 0 do 25, który jest kluczem szyfru Cezara. Dlatego do odszyfrowywania używamy klucza będącego różnica 26 i numeru wiersza.

```
1.  def szyfruj_znak(znak, klucz):
2.      return chr((ord(znak) - ord('A') + klucz) % 26 + ord('A'))
3.
4.  def ktora(litera):
5.      return ord(litera)-ord('A')
6.
7.  def deszyfr(tekst, klucz):
8.      pom = ""
9.      dl = len(klucz)
10.     for i in range(len(tekst)):
11.         k = ktora(klucz[i % dl])
12.         pom = pom + szyfruj_znak(tekst[i], 26 - k)
13.     return pom
```

Testy

```
deszyfr("L","K")
```

wynik "B"

```
deszyfr("H","S")
```

wynik "P"

```
deszyfr("UABMOYDRTSQUDFPPOFLBVWWWYHTGLBAEC","HASLO")
```

wynik "NAJBARDZIEJULUBIONANOWELKATOANTEK"

```
deszyfr("GASOEGUYMDYIFZOMHNJASLVKOZICUSGID","TAJNEPRZEZPOUFNE")
```

wynik "NAJBARDZIEJULUBIONANOWELKATOANTEK"

```
deszyfr("KPVHOPUAMTUZFRYZEKWDEJPBIJ","KOTEK")
```

wynik "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

```
deszyfr("KPVHOPUAMTUZFRYZEKWDEJPBIJ","KOTEKKOTEKKOTEKKOTEKKOTEKKKKKKKK")
```

wynik "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

```
deszyfr("A","KLUCZTOZABEZPIECZENIETEGOSZYFRU")
```

wynik "Q"

```
deszyfr("CKSHQHKZNJIITAXEHIXIAXMFOOHCWRNKUYOMBQD","KLUCZTOZABEZPIECZENIETEGOSZY
FRU")
```

wynik "SZYFROWANIEJESTCIEKAWEIZAWIERATAJEMNICE"

```
deszyfr("ACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSR
TVUWYXZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRT
VUWYXZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTV
UWYXZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVU
WYXZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUW
YXZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWY
XZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYX
ZBACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYXZ
BACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYXZB
ACEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYXZBA
CEDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYXZBAC
EDFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKMLNPOQSRTVUWYXZBACE
DFHGIKJLNMOQPRTSUWVXZYACBDFEGIHJLKMONPRQSUTVXWYAZBDCEGFHJIKML","ABC")
```

wynik
"ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZA
BCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZAB
CDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABC
DEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCD
EFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDE
FGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF
GHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFG
HIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGH
IJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHI
JKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJ
KLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJK
LMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKL"