

PYTHON

22. Cézarova šifra

Vypracovala: Ing. Eva Gabonayová

Predmet: Informatika

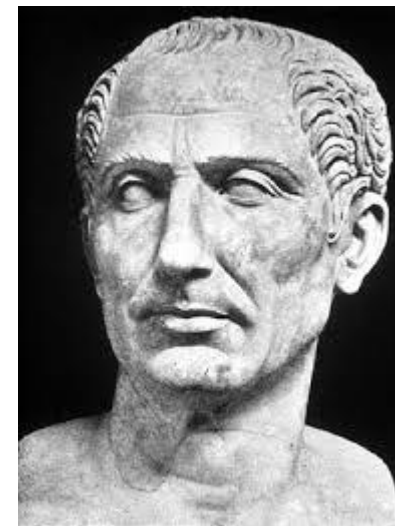
Vzdelávacia oblasť: Matematika a práca s informáciami

Dátum spracovania: 7. 11. 2018



Cézarova šifra

- Caesarova šifra je jednoduchou substituční šifrou, ktorej princíp spočíva v **posune** každého písmena textu o konštantný počet miest v abecede.
- Aj keď sa v dobe Julia Caesara používala len varianta **posunu o 3 písmena**, tak sa názov Cézarova šifra používa pre všetky varianty tohto šifrovacieho systému.



Cézarova šifra

abcdefghijklmnopqrstuvwxyz (vstupná abeceda)
bcdefghijklmnopqrstuvwxyza (prislúchajúce písmeno s posunom 1)

abcdefghijklmnopqrstuvwxyz (vstupná abeceda)
cdefghijklmnopqrstuvwxyzab (prislúchajúce písmeno s posunom 2)

96	`	112	p
97	a	113	q
98	b	114	r
99	c	115	s
100	d	116	t
101	e	117	u
102	f	118	v
103	g	119	w
104	h	120	x
105	i	121	y
106	j	122	z
107	k	123	{
108	l	124	
109	m	125	}
110	n	126	~
111	o	127	DEL

dĺžka abecedy je 26

Cézarova šifra

```
if 'a' <= znak <= 'y':  
    novyznak = chr(ord(znak)+1)  
if znak == 'z':  
    novyznak = 'a'
```

abcdefghijklmnopqrstuvwxyz (vstupná abeceda)
bcdefghijklmnopqrstuvwxyza (prislúchajúce písmeno s posunom 1)

zuzana

avabob

1

Cézarova šifra - algoritmus

```
if 'a' <= znak <= 'z':  
    novyznak = chr( (ord(znak) - 97 + posun) % 26 + 97)
```

% mod zvyšok po celočíselnom delení 26 – dĺžka abecedy

```
abcdefghijklmnopqrstuvwxyz (vstupná abeceda)  
cdefghijklmnopqrstuvwxyzab (prislúchajúce písmeno s posunom 2)
```

zuzana

bwbcpc

2

cxcdqd

3

Čo urobí tento program?

```
#Cézarova šifra
vstup = input('Zadaj text:')
posun = -3
sifra = ''
for znak in vstup:
    novyznak = znak
    if 'a' <= znak <= 'z':
        novyznak = chr( (ord(znak) -
97+posun)%26 + 97 )
    sifra = sifra+novyznak
print(sifra)
```

Domáca úloha

- e-učebnica: Peter Kučera:
Programujeme v Pythone, učebnica informatiky pre SŠ, str. 19,
- otázky 23 - 24 zodpovedať
- úlohy 25-28 vyriešiť, napísať komentáre

Zdroje:

- e-učebnica: Peter Kučera: Programujeme v Pythone, učebnica informatiky pre SŠ
- Python <http://input.sk/python2017/06.html>
- Interaktívny Python

Ďakujem za pozornosť!

