Substituční šifry

Posuny v abecedě

Caesarova šifra = posun v abecedě o 3 pozice

Zašifrujte: `strom`

Dešifrujte: `NRVPRQDXW`

Šifrovací tabulka:

```
abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Příklad: `hledejpodlipou`
`KOHGHMSRGOLSRX`

ROT13 = posun o 13 pozic

Dešifrujte: `ZENXBQENC`

Připravte si sami šifrovací tabulku:

```
abcdefghijklmnopqrstuvwxyz
```

Těžký bonus: Dešifrujte následující zprávu, která používá posun o neznámý počet pozic.

`MLGC KW JMKA DMUAKLFAUA KW BWKLW FWKLAZDA FSKFAVSL`

Substituce s inverzní abecedou

Dešifrujte: `ZOYZGILH`

```
abcdefghijklmnopqrstuvwxyz
ZYXWVUT...
```

Obrázková substituce

Dešifrujte: ⋀⌐⌀□◹⌅⌐○⊔⊥⌶□◹⋕○

```
abcdefghijklmnopqrstuvwxyz
○⌅⋀△⌐⍜⅄⋀⌶⌅⅃□⅄⊔◹⋕◇⋓⌀⊥⅄+⅃⊓⌅⊞
```

Vigenèrova šifra (substituce podle hesla)

Kombinujeme dohromady zprávu a heslo podle „sčítací“ tabulky.

Příklad:

```
hledejpodlipou
slonslonslonsl
ZWSQWUDBVWWCGF
```

Zašifrujte podle hesla **vlk**:

`poklad je v lese`
`vlkvlk . . . . . .`

Dešifrujte pomocí hesla **drak**:

`NFUJHCNSFV`
`. . . . . .`

zpráva

heslo	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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