Táborové šifry crypto

Challenge status: Available
Challenge flags: 6

Ještě chvilku necháme algoritmy a matematiku stranou a podíváme se na klasické táborové šifry, jako například morseovu abecedu, přeskakovačku, hadovku a zónovku. Tyto šifry ukazují, že šifrování může být nejen praktické, ale i zábavné.

232

Theory Flags Handbook Solves

Úvod

Než se vrhneme do čistě matematické a počítačové kryptografie, se pojďme podívat na šifry, které bych nazval "Táborové šifry". To, protože se s nimi nejčastěji setkáte na různých táborech a podobných akcích.

Morseova abeceda

Hovorově "morseovka", anglicky Morse code je způsob komunikace, který se používal hlavně v telegrafii. Celá abeceda včetně čísel je tvořena pomocí teček (`.`) a čárek (`-`) neboli krátkého a dlouhého pípnutí.

Jednotlivá písmena jsou oddělována lomítkem (`/`), slova dvěma lomítky (`//`) a věty třemi lomítky (`///`).

Zde je tabulka písmen a jejich překladu v Morseově abecedě. Zapamatovat si jednotlivé znaky je ze začátku poměrně složité, proto existují pomůcky, jako například slova, která začínají písmenem, které překládají a zároveň jejich slabiky jsou buďto krátké nebo dlouhé podle toho, jestli reprezentují tečku nebo čárku.

A	.-	Akát
B	-...	Blýskavice
C	-.-.	Cílovníci
D	-..	Dálava
E	.	Erb
F	..-.	Filipíny
G	--.	Grónská zem
H	....	Hrachovina
CH	----	Chléb nám dává
I	..	Ibis
J	.---	Jasmín bílý
K	-.-	Krákorá
L	.-..	Lupíneček
M	--	Mává
N	-.	Nástup
O	---	Ó náš pán
P	.--.	Papírníci
Q	--.-	Kvílí orkán
R	.-.	Rarášek
S	...	Sasanka
T	-	Tón
U	..-	Učený
V	...-	Vyučený
W	.--	Wagón klád
X	-..-	Xénokratés
Y	-.--	Ýgar mává
Z	--..	Známá žena
0	-----	

```
1   .----
2   ..---
3   ...--
4   ....-
5   .....
6   -....
7   --...
8   ---..
9   ----.
```

> *U pomocných slov je mnoho variant. Toto jsou ty, pomocí kterých jsem se učil morseovku na táboře já.*

Příklad šifrování - slovo ahoj je: `.-/..../---/.---//`

Napište na papír krátký vzkaz pro vašeho kamaráda nebo spolužáka sedícího vedle vás a pokuste se ho rozluštit.

Advanced Morseova abeceda

V některý případech je šifrování pomocí standardní Morseovy abecedy příliš jednoduché. V tom případě se toho dá s morseovkou dělat opravdu mnoho. Například prohodit tečky a čárky, napsat každé písmeno pozpátku, celý text napsat pozpátku, zapsat morseovku jako čísla, kde prvočísla jsou tečky a ostatní čísla čárky. Morseovka se dá také zapsat jako obrázek (větve na stromě, zuby na pile, trsy trávy...) Možností je opravdu mnoho a je pouze na vaší fantazii, jak daleko morseovku dotáhnete.

Přeskakovačka

Další klasickou táborovou šifrou je přeskakovačka. Na začátku zprávy je nějak definován počet znaků k přeskočení.

Může se jednat o číslo (1): 1B**S**F**K**X**O**W**C**Q**D**Z**O**A**P**H**O**S**L**X**E** (SKOCDOPOLE)

Nebo o písmeno (B --> 2): BAF**S**MZ**K**VR**O**ZA**C**OU**D**RI**O**TO**P**RO**O**ZA**L**IT**E**S (SKOCDOPOLE)

Hadovka

Jak už název napovídá, tak se jedná o šifru, kde je text napsán ve směru nějakého hada

Například ve směru:

```
>---  >---
^  ˇ  |  |
|  |  |  ˇ
O  >--^  X
```

Zašifrovaný text:

```
ODODMNNE
KJHIAENJ
AIANTBEE
LZZUOUTD
VDIKDDEE
```

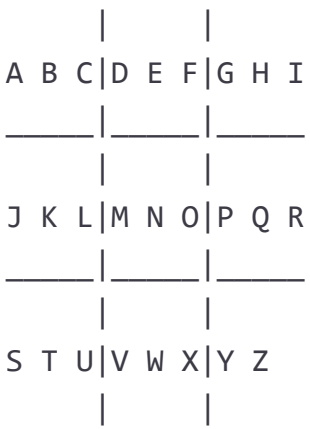
Odšifrovaný text: `VLAKODJIZDIZAHODINUKDOTAMNEBUDETENNEJEDE`.

Variací na směr je mnoho, ale toto pro vysvětlení principu stačí.

Zónovka

Každé písmeno je definováno jako obrázek, udávající jeho pozici v šabloně.

Šablona:



Zašifrovaný text `AHOJ` :

Existuje i její variace, a to s použitím například starého tlačítkového mobilu, jako šablony:

Zašifrované písmeno h

```
_____|
  *  |
_____|
```

Zadání

Představte si, že je horký letní den a jste na táboře. Sešli jste se po skupinkách na nástupu a hlavní vedoucí hlásá: "Budete cestovat po stanovištích, které jsou rozmístěny různě po táboře. Na každém budete muset rozluštit nějakou šifru. Hodně štěstí a... HRA ZAČÍNÁ PRÁVĚ TEĎ!"

Stanoviště č. 1

Dešifrujte text uvnitř závorek: haxagon{ `-/./-.-./-.-/-.--//.-//-.-./.-/.-./-.-/-.--//` }

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

Stanoviště č. 2

Dešifrujte text: haxagon{ `CSUJPUBXOMZWTHZVKMCFAUCAMUXVECMLSKQCEUZBUXDGSACHTZVDRUKOOILMMXARUVGF` }

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

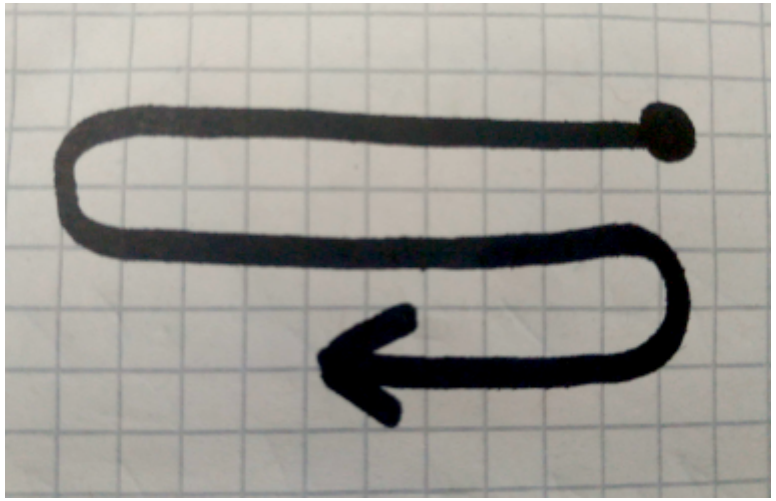
Stanoviště č. 3

Dešifrujte zachycenou telegrafní komunikaci.

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

Stanoviště č. 4



Dešifrujte text:

```
A L K O P
D S E N A
I Z A H C
P O D S T
M E M O R
```

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

Stanoviště č. 5

Dešifrujte text uvnitř závorek: haxagon{ `571/392/817/9//9275/79/4927/1975/9//` }

▶ Nápověda

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

Stanoviště č. 6

Dešifrujte zprávu:

Pro odevzdání vlajky napište text dovnitř závorek, malými písmeny a bez mezer.

> *Příklad formátování: kdyby byl rozšifrovaný text* `pac a pusu`*, tak odevzdáte* `haxagon{pacapusu}`*.*

Stanoviště č. 1

Stanoviště č. 2

Stanoviště č. 3

Stanoviště č. 4

Stanoviště č. 5

Stanoviště č. 6

Flags

01 Stanoviště 1

02 Stanoviště 2

03 Stanoviště 3

04 Stanoviště 4

05 Stanoviště 5