Zkouška náležité kouzelnické úrovně

Kryptologie

Student: Noah Limbani
Profesor: Aki san Marino
Školní rok: Léto 2022

Zadání: **Vlastní šifra**

Syeasmzkuenczfiyozvjktjnsfurjyimnoe.vkesptakriieauiaiupkrAiilzoe,ejlsl

---./.-../---/---./-/./-.--/-/./-//.../.-.-/..././/---/-//-.../-/.--/.-/-./-//-./.-/.../.// ---./.-../../.-../---/-.--/-/./-//.../.-.-/..././/.--/.-.././/../.../----/-.--/..././/-.../--/.//

6130 + 755 + 7 + 919 + 13 - 37 x 00 - 58 + 09 + 0152 : 08 x 028 + 7 + 2 x 6591 x 05 + 967 : 5882 : 1095 x 022 - 4 : 366 + 09 + 0326 x 69 + 888 - 64 - 4010 - 436 + 03 - 4378 : 155 x 861 + 1342 : 40 + 5 x 847 x 12 + 87 x 480 - 58 x 03 - 0824 x 010 + 25 : 328 + 0 - 0223 : 8 - 8227 - 4822 : 939 x 162 + 96 - 6 x 644 : 335 x 001 x 1 x 8 : 5726 x 22 : 2534 + 074 + 84 : 6518 x 63 + 508 x 36 x 6 + 8081 x 260 : 8 x 91 x 24 + 36 : 49 + 632 - 82 =

888 7777 33 1 888 999 6 999 7777 555 33 8 33 1 2 555 33 1 2 8 1 6 2 1 888 999 7 777 2 222 666 888 2 66 444 1 44 555 2 888 88 1 2 1 7 2 8 88 1 2 1 5 33 1 44 666 3 66 33 1 7777 8 88 3 33 66 8 2 1 55 777 999 7 8 666 555 666 4 444 33

medelhzV k uméntun ínávorfišed ,ijudažopen yba ešaV ínávocarpyv olavohasod énečuropod ykléd .ínávocarpz

Pokud by náhodou zadání odolávalo i brutální síle, či narazíte na nejasnosti či nejistotu, napište si směle o nápovědu – není důvodem pro snížení známky. Délka psaného textu by neměla být kratší než 10 palců.

Vypracování:

<~~~~~~~~~~>

Předtím, než se pustím do samotného vypracování zkoušky je třeba vyluštit zadání.

<~~~~~~~~~~>

První šifru jsem odhalila brzy, pro dešifrování je třeba číst jedno písmenko zepředu, pak jedno zezadu a takto postup opakovat.

Zadání:

Syeasmzkuenczfiyozvjktjnsfurjyimnoe.vkesptakriieauiaiupkrAiilzoe,ejlsl

Řešení:

Slysela jsem, ze kouzelnici z Afriky pouzivaji k utajeni sifru krajty pismenkove.

<~~~~~~~~~~>

Druhou šifrou pak byla převrácená morseovka. Tedy čárka je ve skutečnosti tečkou, tečka zase čárkou.

Zadání:

---./.-../---/---./-/./-.--/-/./-//.../.-.-/.../.---/-//-.../-/.--/.-/-./-//-./.-/.../.---./.-../../.-../---/-.--/-/./-//.../.-.-/.../.---/.-../../.---/-.--/.../-...//--/.//

Znaky "správně":

...-/-.--/.../...-/./-/.-.././-/.//---//-.-./---//..././/.---/./-../-./.-/.//.-/-./---//...-/-.--/--/-.--/.../.-.././-/.//---//-.-./---//-.../-.--//--/---/..../.-../---//.---/../-//

Řešení:

vysvetlete o co se jednae ano vymyslete o co by mohlo jit

<~~~~~~~~~~>

Další šifra mi dala trochu zabrat, nakonec jsem ale na způsob dešifrování přišla - v tomto případě se také jedná o Morseovku, sudé číslo je ale tečkou, liché pomlčkou. Matematická znaménka pak dělí jednotlivé písmena od sebe.

Zadání:

6130 + 755 + 7 + 919 + 13 - 37 x 00 - 58 + 09 + 0152 : 08 x 028 + 7 + 2 x 6591 x 05 + 967 : 5882 : 1095 x 022 - 4 : 366 + 09 + 0326 x 69 + 888 - 64 - 4010 - 436 + 03 - 4378 : 155 x 861 + 1342 : 40 + 5 x 847 x 12 + 87 x 480 - 58 x 03 - 0824 x 010 + 25 : 328 + 0 - 0223 : 8 - 8227 - 4822 : 939 x 162 + 96 - 6 x 644 : 335 x 001 x 1 x 8 : 5726 x 22 : 2534 + 074 + 84 : 6518 x 63 + 508 x 36 x 6 + 8081 x 260 : 8 x 91 x 24 + 36 : 49 + 632 - 82 =

Morseovka:

.--./---/-/---/--/--/../-./.-/.--./../.../-/./.---/.-/-.-/-.../-.--/..././-../.-/.-../.-/.../../..-
./.-./.-/.--./---/..-/--../../-/..-/-./.-/.../-./.-/..../.-./.-/.-.././...-/./...-/..../---/-../-
././.../---/..-/-/./--../../.--./.-./../.--./.-/-../-././...-/..././--/../-./.-/.-/.-/..///

Řešení:

potom mi napiste jak by se dala sifra pouzit u nas na hrade ve vhodne soutezi pripadne v seminari

<~~~~~~~~~~>

Čtvrtá šifra odpovídala číslům na mobilu. Jedna skupinka stejného čísla je jedno písmeno a jejich počet odpovídá tomu, kolikrát byste tlačítko na těchto mobilech museli zmáčknout, abyste získali požadované písmeno.

Zadání:

888 7777 33 1 888 999 6 999 7777 555 33 8 33 1 2 555 33 1 2 8 1 6 2 1 888 999 7 777 2 222 666 888 2 66 444 1 44 555 2 888 88 1 2 1 7 2 8 88 1 2 1 5 33 1 44 666 3 66 33 1 7777 8 88 3 33 66 8 2 1 55 777 999 7 8 666 555 666 4 444 33

Řešení:

vse vymyslete ale at ma vypracovani hlavu a patu a je hodne studenta kryptologie

<~~~~~~~~~~>

Poslední šifra pak vyžadovala jednoduché čtení zezadu. Ale pouze po slovech, jejich slovosled je normálně zleva doprava.

Zadání:

medelhzV k uméntun ínávorfišed ,ijudažopen yba ešaV ínávocarpyv olavohasod énečuropod ykléd .ínávocarpz

Řešení:

Vzhledem k nutnému dešifrování nepožaduji, aby Vaše vypracování dosahovalo doporučené délky zpracování.

<~~~~~~~~~~>

Co je tedy mým kompletním zadáním zkoušky?

(přidala jsem háčky a čárky)

Slyšela jsem, že kouzelníci z Afriky používají k utajení šifru krajty písmenkové. Vysvětlete o co se jedná, ano, vymyslete, o co by mohlo jít. Potom mi napište jak by se dala šifra použít u nás na hradě ve ve vhodné soutěži, případně v semináři. Vše vymyslete, ale ať má vypracování hlavu a patu a je hodné studenta kryptologie. Vzhledem k nutnému dešifrování nepožaduji, aby Vaše vypracování osahovalo doporučené délky zpracování.

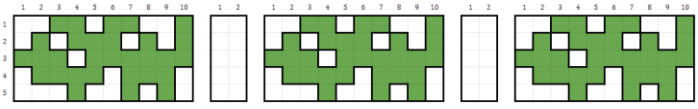
<~~~~~~~~~~>

Abych se pořádně mohla vcítit do života kouzelníků z daleké Afriky, potřebovala jsem si zjistit co nejvíce informací o této krajtě písmenkové. Vycestovala jsem proto do hradní knihovny a dala se do pátrání. Naše knihy sčítají hromadu informací o tomto přenádherném hadovi, rozhodla jsem se ale, že vám zde vytyčím pouze ty nejdůležitější, které mi pomohly při tvorbě šifry.

Krajta písmenková je největším hadem, který se nachází na území Afriky, může mít až 6 metrů. Tento druh je téměř ohrožený, jen zřídka je ale pro člověka smrtelně nebezpečný.

Bylo mi proto jasné, že šifra by to měla být delší a složitější, aby reprezentovala samotnou délku hada a jeho potíže s přežitím. Co mne ale na krajtě zaujalo nejvíce byl vzor, který má na kůži.

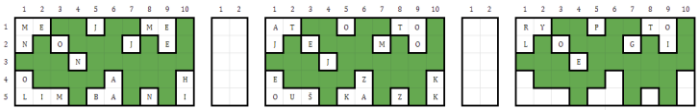
Rozhodla jsem se proto tento vzor aplikovat i na samotnou šifru. Oprášila jsem své znalosti kouzelnického malování a dala se do tvorby vzoru krajty písmenkové. Po nějaké době jsem přišla s blokovým systémem, kde jeden blok byl právě deset čtverečků dlouhý a pět široký. Takový blok by byl jednou z částí klíče šifry, který by se dal opakovat za sebou jak je libo.



(plná velikost)

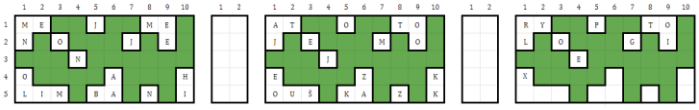
Jak je z obrázku určitě jasné, zelená plocha tvoří vzor krajty písmenkové, jednotlivé bloky jsou pak od sebe odděleny dvěma výplňkovými sloupci. Tento jednoduchý obrázek je tak samotným klíčem k šifře. Do bílých polí u vzoru krajty se po řádcích a blocích napíše váš text, který si přejete zašifrovat.

Pro lepší ukázku jsem se rozhodla zašifrovat text "ME JMENO JE NOAH LIMBANI A TOTO JE MOJE ZKOUŠKA Z KRYPTOLOGIE"



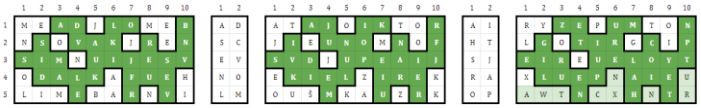
(plná velikost)

Můžete si všimnout, že počet písmen je menší, než je počet bílých ploch. V takovém případě stačí do dalšího bílého pole vepsat písmeno X, které tak označí konec vaší zprávy. To je ale potřeba, aby toto písmeno nebylo užito nikde předtím. Pokud jej ale potřebujete využít, lze se dohodnout na jiném ukončujícím písmenu.



(plná velikost)

A teď už ta lehká část! Stačí do zelených polí a mezer mezi jednotlivými bloky vyplnit "plnící" písmena, která fungují na zmatení nepřítele. Je jedno, jestli písmena vložíte náhodně, nebo se pokusíte tvořit jiné zprávy uvnitř, aby si případný vetřelec myslel, že vyluštil vaši šifru, ačkoli špatně. Takto doplněná písmena mohou vypadat třeba takto:



(plná velikost)

Nyní už máme celou šifru hotovou! Jediné co zbývá je odstranit barvy a spojit jednotlivé bloky dohromady!

(plná velikost)

Celá výsledná šifra tedy může vypadat například takto:

(plná velikost)

Dešifrování s klíčem je pak jednoduché. Můžete si buďto rozdělit šifru zpět na bloky po 10 a 2 jako výplňkové mezery, nebo můžete mít předem vyrobený klíč stávající ze zelené plochy, který jednoduše na papír přiložíte a zbyde vám pouze šifrovaný text.

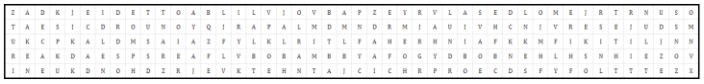
Na této šifře se mi líbí, že jde skládat za sebe a je tak velmi variabilní, co se délky textu týče. Zelenou plochu lze navíc jakkoliv upravit, aby klíč měli jen ti, kterým s klíčem věříte.

<~~~~~~~~~~>

Myslím, že tato šifra má výborný potenciál i pro náš hrad. Seminář by se mi zdál nejvíce vhodný, kdy můžete studentům, podobně jako já vám, ukázat, jak šifra funguje a následně jim zadat za úkol, aby zašifrovali svůj vlastní text, případně dešifrovali nějaký zadaný. Stejně tak by mohlo být za úkol vymyšlení vlastního vzoru, který bude reprezentovat jiné zvíře, ale fungoval by na stejném principu.

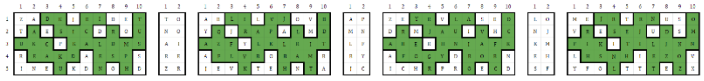
Soutěže si myslím, že by mohly být o něco náročnější na přípravu, jelikož by v každém zadání vyžadovaly vysvětlení, jak šifra funguje, zase by ale takových soutěží mohla vzniknout hromada, kde by pokaždé studenti měli buďto dešifrovat text, nebo případně zašifrovat nějaký vlastní. V šifrovaném textu se zároveň může skrývat i pod úkol, který by se měl k úspěšnému vypracování splnit.

K takovému zadání jsem se pokusila jeden zašifrovaný text připravit. Zašifrované zadání je: ZAJDETE DO PRASINEK DO DABLOVY JAMY A OBJEVTE NAZEV SEDMI HRADNICH PREDMETU SVE USILI VYFOTTE.



(plná velikost)

A samozřejmě vám zasílám verzi i s viditelným klíčem:



(plná velikost)