FRIKONOMIKON
aneb
frikulínské desatero
o pětasedmdesáti bodech

„Co nevyluštíme, ukecáme...
...a co neukecáme,
uběháme.“

1. **První nápady** a **nejjednodušší postupy** bývají často ty správné *(viz. SUD* [1]*, flašky* [2]*...)*.

2. Zkus odhadnout, ke kterému z následujících typů šifer by mohlo zadání patřit. **Smysluplný text** => *steganografie*, *popis cesty* nebo *grafiky*. **Nesmyslný text** => podle frekvenční analýzy buď *substituce* nebo *transpozice*.

Heslo

3. Nemáš nějakého vhodného **kandidáta na klíč**? Zkus použít jako klíč/heslo **názvev hry, název stanoviště, nápovědy** z předchozího průběhu hry**.**

4. Proveď **permutační vyčíslení** klíče. Tj. přiřazení pořadí písmenům v klíči podle pořadí výskytu v abecedě. Může se to dále hodit při pokusech o transpozici.

Základní počty

5. Není toho zhruba **26**? => **Abeceda**.

6. Jsou tam **3 typy** znaků? Mohla by to být nějaká forma **morseovky**, nebo **římské číslice** (I,V,X).

7. Jsou tam **2 typy** znaků ve skupinách po **nejvýše 5** znacích? Mohl by to být zápis v **binární soustavě.**

8. Jsou tam **2 typy** znaků a **2x3** nějakých pozic/rastr? Mohlo by to být **Braillovo písmo**.

9. Není zadání rozděleno na **3(4)** výrazné **části**? Nevyskytují se v něm 3(4) čísla? Není tam něco ve tvaru ***3 prvky – oddělovač – 1 prvek***? Pak by to mohla být **kóta**.

10. Není toho **12**? Neobsahuje to **28 – 31** nějakých **prvků**? => **Kalendář – měsíce, dny.**

11. Nemá to **velikost 8x8**, nebo neobsahuje písmenka a-h a čísla 1-8? => **Šachy.**

12. Není tam něčeho **7/ 52? => Kalendář – dny, týdny.**

13. Není toho **12** nebo **24**? Zkus **hodiny**/zobrazení na **ciferníku hodin**.

14. Nejsou tam **4(8)** různé prvky? - navigace **N**ahoru, **D**olů, **L**evo, **P**ravo, (S, SZ, SV, J, JZ, JV, V, Z) ve 2D a čtení/vykreslování v nějakém rastru.

15. Není tam něčeho **27? => kostka** o rozměrech **3x3x3.**

16 Není tam **6** různých prvků? - navigace **N**ahoru, **D**olů, **L**evo, **P**ravo, Vpřed, Zpět ve 3D.

Substituce

17. Je tam zhruba **26 různých prvků**? Zkus frekvenční analýzu a **substituci**.

18. Jsou tam **běžné znaky abecedy**, ale s divnými frekvencemi výskytu? Mohl by to být nějaký typ substituce:

- ***monoalfabetická šifra*** (Caesar)
- ***homofonní substituce*** – nahrazení jednoho znaku více různými znaky
- ***polyalfabetická šifra*** (Vigenére)
- ***polygramová substituční šifra*** (Playfair)
- ***digrafická susbstituce*** (Polybiův čtverec)

19. Zkus **posun** hrubou silou – všechny varianty.

20. Zkus **posunout text podle** nějakých **zajímavých čísel** vyskytujících se v zadání.

21. **Čísla převeď na písmena**/**písmena převeď na čísla**. Dál pracuj s výsledným textem.

22. Jsou tam nějaké **dvojice znaků/čísel**? Daly by se převést na **desítková**/*šestnáctková* čísla? Mohlo se jednat o **ASCII kód** – intervaly s písmeny: velká **- 65 – 90**/*41 – 5A,* malá **- 97 – 122**/*61 – 7A*

23. Vyskytují se tam **nepísmené znaky**? Mohlo by jít o **kód 1337 – leetspeak** – využití nepísmenných znaků k vyjádření písmen.

24. Vyskytují se tam **zlomky** s malými čísly v čitateli i jmenovateli? Mohlo by jít o **rozdělení abecedy na skupiny**, ve zlomku by bylo zakódováno číslo skupiny a pořadí písmene v ní.

25. Zkus použít **klávesnici mobilu/počítače/T9** – využití znaků z klávesnice k jednoduché substituci *(čísla->písmena, počet stisknutí->písmena...)*, nebo ke grafickému vykreslování znaků do rastru tvořeného klávesnicí.

26. Zkus vypsat vytipované heslo nad zašifrovaný text a provést následující algoritmus pro **dešifrování polyalfabetických systémů**:

- `převeď písmena na čísla 0..25`
- `vyzkoušej pro každou dvojici heslo-šifrový text následující operace:`

systém	**šifrování**	**dešifrování**
Vigenére	O + K = Š	Š – K = O
Varianta Beaufort	O – K = Š	Š + K = O
Beaufort	K – O = Š	K – Š = O

- `if (a+b > 25) then`
  - `return (a+b – 25)`
- `else return (a+b)`
- `if (a-b < 0) then return (a-b + 25)`
- `else return (a-b)`
- `vrácené číslo převeď na písmeno`

27. Vyskytují se v textu opakovaně **dvojice pouze několika málo (5-6) písmen**? Mohlo by se jednat o využití **převodové tabulky s abecedou**, kde by tato písmena tvořila souřadnice. (ADFGX, ADFGVX, MOTUX)

Transpozice

28. Zkus si zadání **pořádně sepsat** – *symetricky/pod sebe/vedle sebe* a systematicky projdi jednotlivé ***sloupce, řádky a úhlopříčky,*** zda neobsahují další část šifry nebo řešení.

29. Zkus přečíst některé části zadání **pozpátku**, **zepředu/zezadu**.

30. Nebyl text rozdělen na **poloviny/třetiny/čtvrtiny** a potom nějakým způsobem prolnut/promíchán?

31. Není text zašifrován **podle plotu** – lichá a sudá písmena na samostatných řádcích a řádky spojeny do jednoho?

32. Nedalo by se využít nějaké **tabulky/obrazce/jiného rastru** ve kterém by byl zapsán otevřený text? Šifrový text by byl vypsán po řádcích/sloupcích, případně složitějším způsobem – spirálou, cik-cak...

33. Nemohla by to být **transpozice podle klíče**? Můžeme zkusit provést následující algoritmus:

- **if** máme kandidáta na klíč
  then provedem permutační vyčíslení a dešifrování textu
- **else**
  - **repeat**
  - určíme možné rozměry tabulky podle délky textu a možných dělitelů
  - zkontrolujeme správnost tabulky
  - **if** poměr samohlásky : souhlásky = 40 : 60
    - **then** rozstříháme sloupce a permutujeme s cílem nalézt vhodné bigramy a rozumné střídání souhlásek a samohlásek ve všech řádcích najednou

34. Nemohla by se využít **Fleissnerova otočná mřížka**? Nemáme k dispozici v zadání/jiných herních materiálech čtverec/mřížku, kde čtvrtinu políček tvoří otvory/označená místa? Pak můžeme zkusit otáčet mřížkou o 90° a číst ve vystřižených polích.

35. Nemohla by to být **transpozice podle Roche**? Máme k dispozici heslo. Určíme permutační vyčíslení. Vyznačíme posloupnost bloků příslušné délky. Do bloků vypíšeme zašifrovaný text. Z bloků postupně čteme otevřený text – vždy první písmeno, po přečtení odmažeme.

Steganografie

36. Zkus přečíst **první/poslední/prostřední/sudá/lichá/x-tá**... písmena/slova/věty z y-tých slov/vět/odstavců.

37. Zkus **odpočítat písmena/slova** v textu podle nějakých zajímavých čísel vyskytujících se v zadání.

38. Zkus v textu najít **zajímavá písmena/znaky** a číst písmena za nimi následující. Zajímavá jsou např. písmena kompletní abecedy, jinde získaného hesla, známé fráze *(Máš IQ větší než 150?...)*, názvu hry, písmena nehodící se do okolního textu *(méně frekventovaná fxwq, s diakritikou...)*.

39. Není součástí zadání nějaká mřížka s otvory? Nezískal jsi ji někde dříve? Případně nemáš k dispozici vhodný text *(pravidla hry, text zadání, text hymny...)*, kam takovou mřížku přiložit? Mohla by to být **Cardanova mřížka**.

40. Děti, **zazpíváme si!** Kdo neumí, může **recitovat...** Nedá se v tom rozpoznat *text známých písniček, básniček, hymny*? A nějak se v textu dál navigovat, nebo vybírat písmena?

41. Když už nepomáhá nic, **pomodli se** ke správnému bohům (využití *textu modliteb, náboženských textů – Bible* apod. k výběru písmen řešení)

Grafika

42. Zkus metodu **kouknu a vidím**.

43. Nemohou být něco v zadání vyjádřené **souřadnice** nebo **rastr**?

44. Nedá se v zadání **něco pospojovat**? ***Posloupnost čísel, písmen, stejné prvky***, ***doplnění*** nějakých ***logických řad***...

45. Zkus si to prohlédnout **proti světlu/prosvítit** baterkou.

46. Zkus se na to podívat **z jiného úhlu**, případně **zašilhat**/**zamhouřit** oči. Mohl by to být stereogram, znetvořené písmo, řeky v textu, nějaké méně nápadné prvky vykreslující grafiku...

47. Zkus **převést znaky na morseovku** – mohla by z toho vylézt **grafika** z teček, čárek a oddělovačů.

48. Nedá se to rozložit na **víc vrstev** nad sebou, tj. Do **3D**?

49. Zkus to zobrazit na nějakém **vhodném displeji/matrici/v digitálních číslech**…

50. Není to **schéma/obrázek/fotka** nějakého zajímavého místa/dalšího stanoviště? Není to **plánek**, nebo zjednodušená/zdeformovaná/zesložitěná **mapa**?

51. Není to **graf**? (Nedá se v něm nalézt nejkratší cesta, neljépe ohodnocená cesta, kořen, cesta mezi stejně/vzestupně/sestupně očíslovanými listy/uzly...?

52. Nedala by se část zadání **překreslit na pauzák** a vhodně ***přiložit/posunovat*** po originálním zadání?

53. Nejde to vhodně **přeložit** a následně prosvítit nebo probodnout špendlíkem?

54. Nejde z toho něco přímo **vystříhat/poskládat/slepit**? Nepomohlo by vystříhání při dalším kroku řešení?

Další typy šifer

55. Není to **popis cesty** k další šifře? Není to popis cesty k nějakému místu v okolí/všeobecně známému místu, které by tě navedlo k dalšímu kroku řešení?

56. Zkus k zadání nalézt **asociace/synonyma/antonyma**. Dál pracuj s nimi.

57. Nelze v zadání vhodně **doplnit** nějaké **řady**? Číselné, písmenné, logické...

58. Pokud jsou v zadání prvky z kalendáře, nedaly by se využít **jména svátků, státní svátky, znamení zvěrokruhu**?

59. Nejsou v zadání nějaké **noty**, **notová osnova** (5 linek), **stupnice**, **akordy**? Nedala by se využít substituce za názvy not/akordů, případně nalézt odpovídající píseň a její text?

60. Zkus si v zadání zahrát **karty** – neodpovídá něco počtu listů, ***očíslování/barvám/označení*** karet?

61. Zkus si v zadání zahrát **šachy** – šachovnice (rozměry 8x8, označení 1-8, A-H), tahy figurek, označení figurek…

62. Nepodobá se zadání nějaké jiné **známé hře**? Není to **sudoku**, **patnáctka**, **sokoban, piškvorky**...? Nedal by se pak průběh hry využít k ***vykreslení/přečtení/získání*** souřadnic řešení?

63. Nevyskytuje se tam několik opakujících se objektů a jejich vlastností? Není to **Zebra** (Einsteinova hádanka)?

64. Není v zadání něco napsaného **neviditelným inkoustem**? Zkus to zahřát nad plamenem/polít peroxidem nebo chemikálií získanou/doporučenou organizátory/prosvítit UV světlem/zářivkou.

65. Není v okolí **nápověda** v podobě nějakých ***zajímavých objektů*** (sud, cívka, vysílač...)/***významných budov*** (radnice)/***ulic***/***pamětihodností*** (pomíky, sochy (sv. Primitivus, ctnosti a neřesti...))?

66. Držíš se opravdu přesně **instrukcí v zadání,** případně v pravidlech hry?

67. Využil jsi už **doporučenou mapu**? ***Souřadnice GPS, zadní strana, legenda, mapové značky, označení čtverců…***

Pro chvíle zoufalství...

68. Porozhlédni se **kolem stanoviště** – nepřehlédl jsi nějakou ***důležitou indicii/organizátora/další části zadání/část šifry*** určenou pouze k obkreslení/prohlédnutí?

69. Opravdu využíváš všechny **dostupné informace**? Tedy vlastní ***zadání šifry***/oficiální ***pravidla hry***/***poslední informace*** před hrou/informace a ***materály ze startovní obálky***/***"nezapomeňte"*** z předchozích šifer/možnosti oficiální ***nápovědy***?

70. Zkus **zpětné inženýrství**… Aneb jak bys se ti mohlo podařit pravděpodobně jednoduchou zprávu, takhle blbě zašifrovat/zamaskovat/zdeformovat?

71. Prohlédni si na mapě dosavadní trasu, odhadni rozumnou vzdálenost, směr a oblasti a **zkus vybrat sympatické místo**, kam se dá rozumně dojít/dojet, které není nijak oplocené/chráněné/jinak nedostupné a nachází se u nějakého zajímavého/význačného bodu a **zkus ho napasovat na zadání**.

72. Když nevíš, najez se.

73. Když víš a máš hlad, představ si, že nevíš, a nejdřív se najez ;).

74. Zkuste se projít kolem, zatancujte si, přesuňte se luštit někam jinam…

75. Zkus využít **pendrekovou kryptoanalýzu** – *„Jedná se o zisk klíče a dalších informací k používanému šifrovému systému, ale tentokrát se využívá vydírání, vyhrožování, mučení."* [3] Ale pozor! Pravidla většiny her a zákony hostitelské země tuto sofistikovanou metodu luštění dost často neumožňují. Je potřeba se před startem hry řádně informovat, případně si zajistit dobrého právníka.

A univerzální rada na závěr od Franty Vomáčky: ***„Když nevíš, derivuj!"***

Zdroje

[1] – 10. šifra, Svíčky 2007
[2] – 7. šifra, Osud 2008
[3] – Pavel Vondruška – Kryptologie, šifrování a tajná písma, Albatros, 2006