Rozličné peňaženky 1

Bezpečnosť nezoradeného semiačka 2

Malý pokus, 5 predmetov 2

Koľko trvá prelomiť 10 slovné semiačko? 3

Abstrakcia 3

Slová navyše 4

Poďme sa porozprávať o bezpečnosti

Bezpečnosť vo svete kryptomien je plne v správe každého jedného človeka. S kryptomenami treba byť rovnako prezieravý ako s čímkoľvek cenným.

Bitcoinová peňaženka je mierne zavádzajúci názov, pretože navodzuje pocit ako keby vaše bitcoiny boli priamo v nej, podobne ako sú vaše eura, karty a doklady v koženej peňaženke vo vrecku vášho kabáta.

Nie je to však tak. Bitcoiny sa nachádzajú v blockchaine, co je zoznam všetkých transakcií ktoré sa v minulosti udiali. U vás v peňaženke sa však nachádzajú dve veľmi dôležité veci.

Hovorí sa im kľúče a slúžia na to aby ste mohli s tými svojimi bitcoinmi narábať. Sú dva:

* Verejný kľúč
* Súkromný kľúč

**Prvý kľúč, verejný** slúži na to aby ste mohli od iných prijímať platby v bitcoinoch. Je to dačo ako číslo účtu v banke. Ak chcete od iných osôb prijímať peniaze, musíte verejný kľúč zverejniť. Súkromný **kľúč** slúži na to aby ste naopak mohli svoje bitcoiny posielať iným luďom. Čiže je to rovnako citlivá informácia ako prihlasovacie údaje do internetbankingu alebo vaša platobná karta. Bitcoinova peňaženka je len úložiskom týchto dvoch kľúčov. Rozličné peňaženky môžu poskytovať aj ďalší komfort, ale základná funkcia je správa kľúčov, informácia o tom, koľko bitcoinov v blockchaine máte, príjem platby pomocou verejného kľúča, vykonanie platby (pomocou súkromného kľúča)

## Rozličné peňaženky

Je úplne na vás akú peňaženku používate, ale mali by ste presne rozumieť z akých možnosti si môžete vybrať. Teraz uvediem 4 základne druhy peňaženky od tej najmenej bezpečnej až po najbezpečnejšiu.

1. **Online peňaženka**, klúče od nej sa nachádzaju kdesi na servri na internete, alebo klaude ako sa dnes hovorí.
2. **Mobilná peňaženka,**
3. **Peňaženka na počitači**,
4. **Peňaženka na špecialnom zariadení**. Toto zariadenie je bežňe vypnute a nepripojené k internetu. Kľúče sú teda prístupne len krátku dobu keď zariadenie pripojíte na elektrinu a internet
5. **Chladná peňaženka**. To je kus papiera kde máte zapísaný privátny kľúč a je napriklad uložený v uzamknutom ohňovzdornom trezore.

Každý, čo sa pohybuje v krypto už nejaký piatok vie, že peňaženku treba mať zazálohovanú aby si človek mohol obnoviť privátny kľúč v pripade nejakej nepríjemnej udalosti. Zálohovanie peňaženky znamená, že chviľu po tom ako si peňaženku nainštalujete vykonáte kroky podľa návodu aby ste v pripade nejakých problémov vedeli obnoviť váš privátny kľúč do inej peňaženky. Problemom môže byť napríkladt strata mobilu, resetovanie mobilu a následne vymazanie nainštalovaných aplikácii.  
  
Veľmi oblúbená technika zálohovania a obnovy privátneho kľúča je *seed*, čo by sa do slovenčiny najlepšie preložilo ako *semiačko* či *počiatok.* Pretože z neho može opať vyrasť pôvodný stratený kľúč. Pri tejto technike si človek zapíše 12/18/24 slov v takom poradí ako mu ich peňaženka nadiktovala. A keď príde deň že peňaženku treba obnoviť na inom zariadení, tak len zadá tých 12/18/24 slov v správnom poradí a kľúč sa obnoví.

Na koľko je tento postup bezpečný, čiže nenapadnutelný a nakoľko je bezpečna ochrana **60/24**  ktorú ponúka Andrej?

Aká je šanca že v lotérii uhádnem všetky čísla? Kolko zápasov treba odohrať... Takéto príklady rieši kombinatorika - každý sme sa to učili v škole. Určite si pamatate

* *Koľko zápasov sa odohrá na majstrovstvách sveta v hokeji v prípade že:*
  + *v každej zo skupín (A, B po 8 mužstiev) hrá každý s každým jeden zápas bez odvety, čím sa určí číselné poradie v každej skupine...*

Lenže naše pani učiteľky matematiky majú nešťastný zvyk žiakov učiť vzorce miesto toho aby ich učili používať rozum. Takže poďme si to spočítať bez toho aby sme museli hladať na webe vzorce.

## Bezpečnosť nezoradeného semiačka

Predstavme si, že sme si urobili zálohu, mame 24 slov a požiadali sme Andreja aby nám urobil tabulky s jednotlivými slovami. Može to nejako zneužiť? Veď pozná našich 24 slov. Ano, slová pozná, ale nepozná ich poradie. Koľko je možnosti ako tych 24 slov zoradiť, koľko rozličných semiačok z nich možeme poskladať?

Takže čo nám hovorí zdravý rozum? Máme 24 slov a ideme skladať. Prvým môže byť ktorékoľvek slovo, na druhú pozíciu už možeme dať len jedno zo zvyšných 23, na tretiu jedno z prebývajúcich 22... Takže, ideme naostro 24 krát 23 je 552, krát 22 je... Viete čo, vyskúšajme si to najprv na menších číslach.

### Malý pokus, 5 predmetov

Takže, na prvej pozícii môže byť 5 rozličných slov, na druhej

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5x | 4x | 3x | 2x | 1x | => | 5\*4\*3\*2\*1=120 možností |

Z našich 5 nezoradených slov náme 120 možnosti, ale ten lump čo to bude náhodne skladať môže mať štastie a uhádne to už na druhy krat. Čo by bolo keby sme mali 10 slov? Je to take jednoduche, 10 krát 9 krát 8...

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10 | 9 | ... | 2 | 1 | => | 10\*9\*8\*7\*6\*5\*4\*3\*2\*1=3,6 miliona možností |

Naozaj 3 miliony? Nie je to šialene?

## Koľko trvá prelomiť 10 slovné semiačko?

Koľko by to takemuto brute force hackerovi trvalo prelomiť? Nech vie naozaj rychlo klepať do klavesnice a zadá jednu kombináciu za 10 sekund. Rok má:

365 dní \*24 hodín \*60 minút \* 60 sekúnd = 31 536 000 číže **31 miliona sekund**.

Takže už pri 10 tabuľkách by sa ten hacker dosť natrápil a trvalo by mu to mesiace až rok.

## Abstrakcia

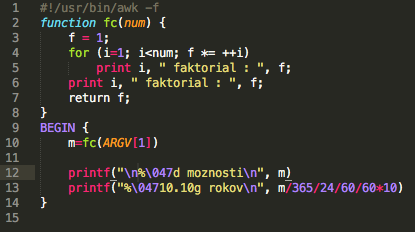
Skúsme teraz urobiť abstrakciu a odhadnúť ako by vzorec vyzeral pre 24 tabuliek:

24\*23\*22\*21\*...2\*1=

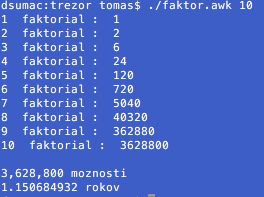
Také číslo sa volá v matematike faktorial a rastie tak rychlo ako si ani predstaviť nedokážete. Tí z vás ktorý vďaka kryptu uverili že je len jeden boh na svete a Kernigham, Ritchi a Torvalds su jeho prorokmi si to možu vyskušať hned teraz.

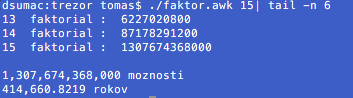
Ako inak, v komandlajne. Pomocou jazyka awk. Awk je prvý tabulkovy procesor na svete ktorý tu bol v dobach keď Bill Gates tahal za sebou káčera a zvedavci si to môžu vyskúšať:

<https://github.com/pay4UU/trezor>



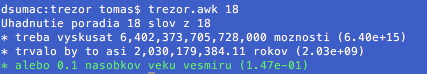
a výsledok?



10 tabuliek, vyše roka lúštenia. Môže to byž vôbec pravda? Čo by spravolo 15 tabuliek?  


Už pri 15 tabulkach by to Andrej lúštil 400 tisíc rokov. Čiže aby vas exploitol, musel by začať v dobe keď na zemi paramamuty.

A pri zazálohovani 18 slov by to trvalo 1/10 času ktorý uplinul od Veľkeho Tresku

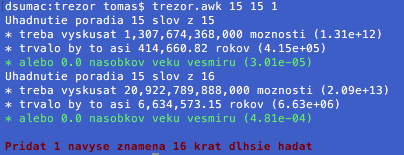


I like Linux. Because linux is like wigwam.

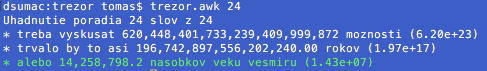
No gates, no windows, just apache inside

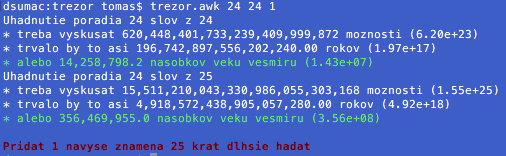
## Slová navyše

Čo by sa stalo keby sme pridali daľšiu tabulku s nezmyselným slovom ktoré do zoznamu nepatrí? To slovo možeme pridať, na začiatok, za prve slovo, za druhe, za tretie... až za 15. Čiže máme ďalších 16 možností. Faktoriál 15 a ešte vynásobiť 16-timi



Poradie 24 slov z 24 by sa hádalo 14 miliard krat dlhsie ako trva tento vesmir od bigbangu po dnes



A keby sme pridali jedno dalšie

, bolo by to 25 krat dlhšie, lebo 25 slovo môžeme pridať bud pred pôvodne prvé, pred pôvodne druhé, pred tretie… pred 24. alebo za 24. Čiže pridávame 25 nových možností