Šifrování

Matematické výpočty

Vypočítejte následující úlohy

1. Kolik existuje možností tvorby hesla pokud:

* se skládá z 5 čísel (0-9) a čísla se smí opakovat [výsledek – 10^5]
* se skládá z 8 písmen abecedy (abcdefghijklmnopqrstuvwxyz a rozlišují se malá a velká) a písmena se nesmí opakovat [výsledek – 30 342 338 208 000]
* se skládá z nejprve 5 čísel (0-9) a pak z 3 písmen abecedy (abcdefghijklmnopqrstuvwxyz a rozlišují se malá a velká) – čísla ani písmena se nesmí opakovat [výsledek – 4 009 824 000]

1. Heslo je dlouhé 6 znaků a skládá se z čísel (0-9), písmen abecedy (abcdefghijklmnopqrstuvwxyz a rozlišují se malá a velká) a speciálních znaků (\_#\*; … - celkem deset), vše se smí opakovat – kolik existuje takto vytvořených hesel? [výsledek – 72^6]
2. Číselný zámek na jízdní kolo se skládá ze 4 pozic čísel. Zloděj dokáže otestovat jednu číselnou kombinaci za 20 sekund. Jaká je nejkratší/nejdelší doba, za kterou nám můžou odcizit kolo?

[výsledek – nejkratší – 0s (kolo nebylo zamčeno), nejdelší 2 dny, 7 hodin, 33minut]

1. „Jednotlivé stolní počítače můžou vyzkoušet více než sto milionů hesel za sekundu použitím různých metod k prolomení hesla, které budou spuštěny na běžném CPU, jak ho známe.“

Zdroj:

Přispěvatelé Wikipedie,*Prolomení hesla* [online], Wikipedie: Otevřená encyklopedie, c2016, Datum poslední revize 7. 07. 2016, 07:57 UTC, [citováno 22. 02. 2018] <<https://cs.wikipedia.org/w/index.php?title=Prolomen%C3%AD_hesla&oldid=13897450>>

Určete nejdelší dobu, která bude potřeba k prolomení hesla, které se bude skládat z 5 znaků (velkých a malých písmen, čísel a speciálních znaků – vše se může opakovat). Jaké existují mechanismy, aby takto rychlému prolomení zabránily? Pro naši potřebu budeme uvažovat, že počítač zvládne vyzkoušet za sekundu přesně sto milionů hesel.

[výsledek – 19,3s, např. po několika chybných pokusech zablokování účtu, nutnost čekat 5 minut před dalším pokusem atd.]