**Šifrování zpráv (M)**

Zadání:

1. Prezentace

a) Vyhledejte informace o tématu kryptografie (konkrétně šifrování zpráv) a vyberte si jednu šifrovací metodu. Výběr proběhne společně s učitelem. Jednu šifrovací metodu následně zpracovávají dva žáci (pracuje se ve dvojicích).

b) Zpracujte prezentaci o vybrané šifrovací metodě.

* Prezentaci zpracujte ve dvojicích.
* Prezentace bude mít všechny náležitosti, které má správná prezentace obsahovat – titulní strana, obsah, vlastní téma prezentace, poděkování za pozornost atd. Nezapomeňte uvést zdroje, ze kterých jste čerpali dle citačních norem!
* Tématem prezentace je nejen samotný princip šifrovací metody, ale ideálně také historické zajímavosti o ní a o jejím použití.

1. Tvorba vývojového diagramu

a) Vyhledejte a vyberte (popř. vymyslete) jednu metodu šifrování zpráv. (Nemusí se jednat o tutéž metodu, pro kterou se připravovala prezentace.)

b) Sestavte pro tuto metodu vývojový diagram. Upřesnění:

* vybranou metodou musí jít jakýkoliv text zašifrovat a potom naopak rozšifrovat;
* kvůli následnému počítačovému zpracování by mělo jít o šifrování textu do textu, případně čísel.

c) Po sestavení si diagramy vyměňte s jiným žákem (výměny určuje učitel) a pokuste se zašifrovat a následně dešifrovat slovo nebo krátkou větu. Porovnejte vstupy a výstupy, a pokud se neshodují, najděte v diagramu chybu a opravte ji. Zkontrolujte diagram i v případě, že se výstupy shodují.

1. Programování

S využitím algoritmu, který jste v minulé úloze vytvořili, vytvořte program, který dokáže šifrovat a dešifrovat zprávy. (Programovací prostředí určuje učitel.)

1. Interpretace algoritmu

Po vytvoření programu vyzkoušejte a zhodnoťte program jiného žáka (výměny určuje učitel). Svými slovy popište, jak funguje kód spolužáka.

1. Matematické výpočty

Vypočítejte následující úlohy:

1. Kolik existuje možností tvorby hesla, pokud:

* se skládá z 5 čísel (0-9) a čísla se smí opakovat;
* se skládá z 8 písmen abecedy (abcdefghijklmnopqrstuvwxyz a rozlišují se malá a velká) a písmena se nesmí opakovat;
* 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;

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?
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?
3. „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.