DUM 9 téma: Caesarova šifra

ze sady: 1 **tematický okruh sady:** Algoritmy a datové struktury
ze šablony: 10 – Algoritmizace a programování **určeno pro:** 1. a 2. ročník
vzdělávací obor: 18-20-M/01 Informační technologie
26-41-M/01 Elektrotechnika - Elektronické počítačové systémy
vzdělávací oblast: odborné vzdělávání
metodický list/anotace: VY_32_INOVACE_10109ml.pdf
pomocné soubory: sifra.cpp, desifra.cpp, original.txt, sifra.txt

I. Problém bezpečného přenosu dat

Největších pokroků v této oblasti dochází během válek (Caesar a jeho šifra, druhá světová válka a Enigma atd.). Jedna strana se snaží vymyslet nerozluštitelnou šifru a druhá strana se jí snaží za každou cenu rozluštit.

a. Proces komunikace – symetrická šifra.

Máme dva komunikující: Alici (A) a Bena (B).
Alice a Ben si domluví nějaký klíč (K).
Alice zašifruje zprávu (Z) klíčem (K) a vznikne zašifrovaná zpráva (Š).
Zašifrovanou zprávu (Š) pošleme Benovi.
Ben přijme zašifrovanou zprávu (Š).
Ben pomocí klíče zprávu (Š) dešifruje, aby získal původní zprávu (Z).

b. Parametry

Velikost klíče .....
Předání klíče .....
Předání zašifrované zprávy .....
Vlastnosti zašifrované zprávy .....

II. Caesarova šifra

Používal ji Caesar pro rozdávání vojenských rozkazů.
Klíč : 3 čísla ***a, b, c***
Zašifrování:

1. znak posunu o ***a*** symbolů.
2. znak posunu o ***b*** symbolů.
3. znak posunu o ***c*** symbolů.
4. znak posunu o ***a*** symbolů.
5. znak posunu o ***b*** symbolů.

é é é

Dešifrování probíhá stejně, akorát se symboly posouvají opačným směrem.

a. Šifrování

Zašifrujte slovo PROGRAMOVANI Caesarovou šifrou klíčem 2 1 3.

b. Dešifrování

Dešifrujte zprávu TQBPVA klíčem 1 2 0.

III. Vyzkoušejte

Program *sifra.exe* zašifruje soubor *original.txt* do souboru *sifra.txt*.
Program *desifra.exe* dešifruje soubor *sifra.txt* do souboru *desifra.txt*.

1) Spusťte program sifra.exe a zvolte klíč 0 1 2 a vyzkoušejte, jak bude vypadat zašifrovaný soubor.
2) Vyřešte úlohy z předchozí kapitoly pomocí programů *sifra.exe* a *desifra.exe* (musíte změnit obsah souborů *originál.txt* a *sifra.txt*).
3) Zašifrujte pomocí programu *sifra.exe* nějakou zprávu a pošlete ji mailem dalšímu studentovi ve třídě, který ji dešifruje programem *desifra.exe* (domluvte si tajný kód).

IV. Tvorba programu - Caesarova šifra

Skládá se ze dvou samostatných programů:

a. Šifrování – algoritmus

```
Vstup:    Klíč (K) - tři čísla
          Zpráva (Z)
Výstup:   Šifrovaná zpráva (Š)
```

b. Dešifrování – algoritmus

```
Vstup:    Klíč (K) - tři čísla
          Šifrovaná zpráva (Š)
Výstup:   Zpráva (Z)
```

c. Program

Šifrování i dešifrován probíhá stejným způsobem. Liší se pouze posun znaků. V případě šifrování posouváme znaky dopředu (přičítáme klíč) a v případě dešifrování posouváme znaky dozadu (odečítáme klíč).

Jádro programu (šifrování):

```
while((znak=getc(f))!=EOF){
   switch(pocet%3){
     case 0:znak=znak+a; break;
     case 1:znak=znak+b; break;
     case 2:znak=znak+c; break;
   }
   putc(znak,g);
   pocet++;
 }
```

d. Možné problémy při šifrování

Překročíme rozsah ASCI tabulky – musíme zkontrolovat, zda se číslo nachází v ASCI tabulce. V programu ověřujeme podmínkou **`if (znak>255)`**.

Zašifrovaná zpráva obsahuje nepovolené znaky (konec souboru, pípnutí atd..). V našem programu toto není ověřeno a tajně doufáme, že na tyto znaky nenarazíme. Vyřešit to můžeme tak, že po znaku Z bude následovat opět znak A (nutno ověřit podmínkou).