

Jméno:

ZKOUŠKA

Šifrování

2. stupeň

Šifrovací kříže

Tento filtr přeuspořádává vložený text podle pravidel šifrovacích jednoduchých křížů. Nejprve si představme, že se vypíše text po skupinkách po čtyřech do kříže. První písmeno je v kříži vlevo, druhé nahoře, třetí vpravo, čtvrté dole (začíná se zleva po směru hodinových ručiček). Těchto kruhů je vedle sebe napsáno tolik, kolik jich je potřeba pro zapsání celé šifry. Takovýto text se potom přečte po řádcích a to je výsledná šifra.

Úkolem bude:

- Přečtení zašifrované zprávy
- Zašifrování zprávy bez chyby



Šifrování

Nejprve si text rozdělíme do skupinek po čtyřech písmenech. Tyto písmena pak rozepíšeme po křížích vedle sebe, kde do každého cípu kříže umístíme jedno písmeno. V každém kříži začínáme vlevo a pokračujeme po směru hodinových ručiček. Až takto zapíšeme celou zprávu, pak ji přečteme po řádcích. Do zprávy případně zapisujeme i mezery, které vznikly při nedokončení posledního kříže, jinak by takováto šifra byla jen těžko luštitelná.

Příklad: chceme zašifrovat slovo ZELENINA:

1) Rozvrhneme si písmena po čtyřech:

zele nina

2) Představíme si kříže a jejich čtyři cípy, kam budeme umisťovat písmena:

```
*      *
*  *  *  *
*      *
```

3) Do každého cípu pak zapíšeme jedno písmeno. Začínáme zleva a postupujeme po směru hodinových ručiček. Obecný postup je podle čísel v následujícím schématu:

```
  2      6
1  3  5  7
  4      8
```

4) Podle výše uvedených pravidel zapíšeme do křížů opravdovou zprávu:

```
  E      I
Z  L  N  N
  E      A
```

5) Výsledek přečteme po řádcích, takže v našem případě vyjde:

EIZLNNEA

Dešifrování

Nejdříve zjistíme počet písmen a vydělíme ho číslem 4. Tím jsme přišli na počet křížů, takže si rozvrhneme pro ně místo. Celou první čtvrtinu napíšeme jako kdyby vždy jen do vrchního cípu každého kříže. Další polovinu textu zapíšeme vždy střídavě do levé a pravé části každého kříže postupně. Zbylou čtvrtinu textu zapíšeme do dolní části křížů.

Ukažme si to na příkladu. Dostali jsme zašifrovanou zprávu EIZLNNEA:

1) Šifrovaná zpráva má 8 písmen, takže na zašifrování byly potřeba dva kříže. Vytvoříme si dostatek místa pro tyto kříže:

```
*      *
*  *  *  *
*      *
```

2) Do horních cípů zapíšeme první dvě písmena (E,I):

```
E      I
*  *  *  *
*      *
```

3) Následující polovinu textu (4 písmena) použijeme vždy pro levý a pravý cíp (Z,L,N,N):

```
E      I
Z  L  N  N
*      *
```

4) Zbylou čtvrtinu textu (2 písmena - E,A) doplníme postupně do poslední části křížů:

```
E      I
Z  L  N  N
E      A
```

5) Teď nám vyšlo stejné schéma, jaké bylo zřejmě použito při šifrování, takže nám už nic nebrání, abychom si přečetli. Čteme kříž po kříži, v každém kříži začínáme v levém cípu a pokračujeme po směru hodinových ručiček. V našem případě tedy vyjde jako dešifrovaný text ZELENINA.

| Úkol | Splněno |
|-----------|---------|
| Přečtení | |
| Šifrování | |

Mobilová šifra

Tento filtr přebírá jako vstup nějaký text a do výstupu vkládá číslice tak, jak by se mačkali při vkládání textové zprávy do mobilního telefonu.

Úkolem bude:

- Rozšifrovat zprávu bez nápovědy
- Zašifrovat zprávu bez nápovědy a BEZ CHYBY



Šifrování

Šifrování touto šifrou je velice jednoduché. Každý, kdo již někdy posílal nějakou krátkou textovou zprávu na mobilním telefonu, jistě poznal tento jednoduchý způsob. Každé jednotlivé písmeno se šifruje tak, že se vždy napíše číslo tlačítka tolikrát, kolikáté je dané písmeno na daném tlačítku zobrazené. Jako mezera se používá číslo 1.

| Úkol | Splněno |
|-------------|---------|
| Přečtení | |
| Zašifrování | |

Zlomková šifra

Tato šifra šifruje daná písmena abecedy tak, že je nahrazuje zlomky. Protože je k dispozici pouze 25 písmen, pak písmeno W není touto šifrou zpracovááno. Stejně tak písmeno Ch je bráno jako dva na sobě nezávislé znaky C a H.

Úkolem bude:

- Zašifrovat zprávu
- Rozšifrovat zprávu

Šifrování

Pokud šifrujeme, měli bychom si napsat, které písmeno je vyjádřeno jakým zlomkem. Nejprve si napíšeme abecedu bez Ch a bez W. Nejlépe uděláme, pokud za každou pěticí vynecháme trochu místa. Pomůže nám to potom při šifrování. Pod toto abecedu napíšeme pětkrát za sebou čísla od jedné do pěti. Těchto 25 čísel vyjadřuje čísel. A podtrhneme vodorovnou čarou, která pak bude vyjadřovat zlomkovou čáru. Vznikne asi toto:

```
ABCDE FGHIJ KLMNO PQRST UVXYZ
12345 12345 12345 12345 12345
-----
```

Pod každou pěticí písmen a čísel napíšeme číslo od 1 do pěti. Těchto pět čísel pak vyjadřuje jmenovatel. Výsledek je pak tento:

```
ABCDE FGHIJ KLMNO PQRST UVXYZ
12345 12345 12345 12345 12345
-----
   1     2     3     4     5
```

Pokud jsme provedli takovouto přípravu, pak šifrování je již jednoduché. V takovéto tabulce pak nalezneme písmeno, které bychom chtěli zašifrovat. Do čitatele napíšeme číslo, které se nachází pod vyhledaným písmenem. Oddělíme zlomkovou čarou a jako jmenovatel napíšeme číslo, které je pod tou pěticí čísel, ke které náleží naše šifrované písmeno. Takto postupujeme až do konce šifry.

Dešifrování

Pokud jsme si udělali přípravu jako při šifrování, pak při dešifrování postupujeme přesně opačně.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | X | Y | Z | | | | | |
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| | | 1 | | | | | 2 | | | | | 3 | | | | | 4 | | | | | 5 | | | | | | | |

| Úkol | Splněno |
|-------------|----------------|
| Zašifrování | |
| Rozluštění | |

| Druhá úroveň zkoušky | Splněno |
|-----------------------------|----------------|
| | |