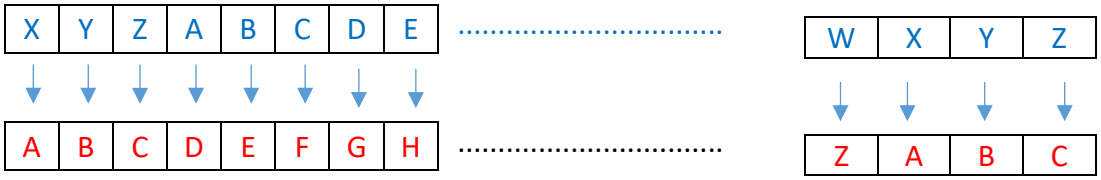
Dům dětí a mládeže Ostrava-Poruba příspěvková organizace

**středisko DDM Polská**
Polská 1624/4, Ostrava – Poruba 708 00
www.ddmporuba.cz

## Pracovní list číslo 1: SUBSTITUČNÍ ŠIFRY

Substituce znamená nahrazení. Jeden prvek se nahradí za jiný. Třeba jedno písmeno číslem, slovo obrázkem a podobně.
Tento princip je velmi starý. Používali ho už Římané. Gaius Julius Caesar (100 př. n. l. - 44. př. n. l.) posouval písmena v abecedě o tři pozice (svou metodu popsal v Zápiscích o válce galské). Písmeno A se zamění za D, písmeno B za E a tak dále.




Abeceda se používá cyklicky, tedy jako kdyby za písmenem Z začínala znovu od A. Této šifře se pak říká posun nebo Caesarová šifra.
Princip substituce použijeme při kódování: Například nahrazením písmene K za morseovkový symbol – · – nebo zaměnění symbolu  za písmeno A.
Oblíbenou možností je šifrování podle domluveného klíče: Domluvíme se, čím bude které písmeno nahrazeno. Příkladem je použití známého Polybiova čtverce, tabulky 5 x 5, do které se vepíši písmena abecedy a pak se udávají jejich souřadnice.

## ŠIFRY

**Posun o 2 písmena *** B G T Y B J M

**Převrácená abeceda **** N Z G V I R W L F H P Z
(nápověda: $A \rightarrow Z; B \rightarrow Y$)

**Polybiův čtverec ****

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

zadání:

31 24 32 34 33 11 14 11

**Jméno v tajném písmu ****

| | |
|---|---|
| Δ ∃ $X$ ∩ ¬ ∇ | MICHAL |
| Δ ¬ ~ ∗ ∃ ∞ | MARTIN |
| ∇ ∝ $X$ ∃ ∅ | LUCIE |
| ∪ ¬ ∗ ∅ ~ ∃ ∞ ¬ | KATERINA |
| ∗ ∀ Δ ¬ $\epsilon$ | TOMAS |
| ∩ ~ ∀ Δ ∞ ∃ $X$ ∅ | ? |

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

OSTRAVA!!!

| **Přezdívka** | **Jméno** | **Příjmení** | **Věk** (např. 10 let) | **Kontakt** |
|---|---|---|---|---|
| | | | | |
| **Obtížnost** | **Název** | **Řešení šifry** | | **Počet bodů** |
| Lehká * | Posun o 2 písmena | | | |
| Střední ** | Převrácená abeceda | | | |
| Střední ** | Polybiův čtverec | | | |
| Střední ** | Jméno v tajném písmu | | | |

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz