Interreg
EVROPSKÁ UNIE
Rakousko-Česká republika
Evropský fond pro regionální rozvoj

| Tento výukový materiál byl vytvořen v rámci projektu MatemaTech – Matematickou cestou k technice | |
|---|---|
| Předmět: | Matematika |
| Téma: | Základní substituční šifry |
| Věk žáků: | 8 -19 let |
| Časová dotace: | 1 - 2 vyučovací hodiny |
| Potřebné pomůcky, požadavky na techniku: | - dataprojektor pro učitele<br>- možnost kopírovat pracovní list |
| Požadované znalosti a dovednosti žáků: | - základní kombinatorické schopnosti<br>- schopnosti orientovat se v tabulce<br>- intuitivní znalosti souřadného systému v rovině |
| Získané dovednosti a znalosti: | - seznámení se se základními principy šifrování |
| Aplikace tématu v reálném životě: | - žák může využít znalostí k psaní a čtení šifrovaných zpráv<br>- žák si procvičí trpělivost |
| Zdroje: | - Mendelova univerzita v Brně, https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7023<br>- Michal Musílek, Univerzita HK, http://musilek.eu/michal/sifry<br>- Wikipedie:<br>- https://cs.wikipedia.org/wiki/Homofonn%C3%AD_%C5%A1ifra<br>- https://sk.wikipedia.org/wiki/Atba%C5%A1 |
| Autor: | Mgr. Marek Vejsada |

# ŠIFROVÁNÍ – ZÁKLADNÍ INFORMACE

## 1. Co je to šifrování?

Šifrování je proces, při kterém se snažíme upravit daný text tak, aby ho byl schopen přečíst pouze ten, kdo zná šifrovací klíč, tedy způsob, kterým byl původní text převeden.

## 2. Substituční šifra

V tomto druhu šifrování dochází k záměně písmena abecedy za jiné písmeno či znak. Pokud používáme pro zakódování zprávy pouze jednu abecedu, hovoříme o monoalfabetické šifře. Pokud je použito abeced více (uspořádaných do tabulky), jedná se o polyalfabetické šifry.

## 3. Caesarova šifra

Caesarova šifra patří mezi nejznámější substituční monoalfabetické šifry. Je stará více než 2000 let a jedná se zřejmě o nejslavnější šifru. Šifrovací klíč spočívá v tom, že pod abecedu napíšeme abecedu šifrovací posunutou o několik znaků vpravo. Číslo udávající posun abecedy je šifrovací klíč. Kdybychom použili číslo 3[1], vypadala by Caesarova šifra takto:

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

Zašifrovat otevřený text (tedy text, který chceme zakódovat), je jednoduché. Každému písmenu otevřeného textu v první řádce přiřadíme písmeno v řádce druhé. Při dešifrování se postupuje obráceně.

## 4. Šifra ATBAŠ

Tato substituční šifra je monoalfabetická. Vznikla asi 500 let před Kristem a prokazatelně ji poprvé používali hebrejci. Šifrovací klíč je dán tím, že se ve druhé řádce napíše abeceda pozpátku. Odtud pochází také její název – podle prvních a posledních písmen hebrejské abecedy (1 – **a**lef, 22 – **t**av, 2 – **b**eit, 21 – **sh**in). [3]

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

## 5. Šifra se slovním klíčem

Substituční monoalfabetickou šifru můžeme zadat také tak, že použijeme slovo, které známe pouze my a ten, co zprávu dešifruje. Toto slovo nemusí mít žádný jazykový smysl. Napíšeme jej na začátek druhého řádku tabulky a dopíšeme zbývající písmena abecedy, která se v klíčovém slově neobjevila. Pokud by se v klíči některá písmena opakovala, vyškrtli bychom je. Tak například z klíčového slova „KYTKA“ by se stalo klíčové slovo „KYTA“. Druhé „K“ v klíči bychom museli vypustit, protože

[1] Tuto šifru (pro posun o tři místa doprava) používal Caesar. Odtud plyne její název.

jinak by ve druhé řádce tabulky chybělo písmeno „Z“ a nevěděli bychom, jak dešifrovat písmeno „K“, protože by se v tabulce ve druhé řádce vyskytovalo dvakrát. Použijeme-li klíčové slovo „KYTZA“, bude šifrovací tabulka vypadat takto:

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

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

## 6. Vigenérova šifra

Tentokrát se jedná o polyafabetickou šifru z roku 1586. Abecedu uspořádáme do tabulky (Vigenérův čtverec, tzv. tabula recta): [4]

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

Poslední řádka tabulky je opět abeceda od písmene „A“. Je to kvůli rychlejší a pohodlnější orientaci ve schématu.
Šifra využívá klíčové slovo, které se opakovaně napíše nad otevřený text. Zvolme pro ukázku klíčové slovo „TECHNIKA“ a otevřený text „DNES JE KRÁSNÝ DEN“. Otevřený text napíšeme do druhé řádky tabulky a klíčové slovo do první řádky opakovaně:

| T | E | C | H | N | I | K | A | T | E | C | H | N | I | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | N | E | S | J | E | K | R | A | S | N | Y | D | E | N |

Způsob šifrování:
První písmeno otevřeného textu je „D“, odpovídající písmeno klíče nad ním je „T“. Ve Vigenérově čtverci najdeme průnikové písmeno odpovídající sloupci „D“ a řádce „T“. V tomto případě šifrujeme písmenem „W“.

| T | E | C | H | N | I | K | A | T | E | C | H | N | I | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | N | E | S | J | E | K | R | A | S | N | Y | D | E | N |
| W | S | G | Z | W | M | U | R | T | W | P | F | Q | M | X |

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

Při dešifrování postupujeme tak, že si vybereme písmeno klíče a v tabulce vyhledáme řádek začínající tímto písmenem. V tomto vybraném řádku najdeme písmeno šifrovaného textu a první písmeno příslušného sloupce je hledaný znak otevřeného textu. Jako příklad bychom mohli použít dvojici „N“ a „W“, která nás přivede ke znaku „J“:

| T | E | C | H | N | I | K | A | T | E | C | H | N | I | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| W | S | G | Z | W | M | U | R | T | W | P | F | Q | M | X |
| | | | | J | | | | | | | | | | |

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

# 7. Playfairova šifra

Autor šifry je Charles Wheatstone, proslavil ji Lyon Playfair, po němž dostala své jméno. Tato šifra nahrazuje každou dvojici písmen v otevřeném textu jinou dvojicí písmen. Jedná se o polygramovou substituční šifru, ve které se nahrazují skupiny písmen (dvojice – digramy, trojice – trigramy, …) [1], [5].

Playfairova šifra pracuje s digramy. Je to šifra, která používá klíč. Klíč je jakýkoliv řetězec písmen, ve kterém se písmena neopakují. Pokud ano, ty opakující se vyškrtávají stejně, jako v kapitole 5.

Pro konkrétní příklad vyberme klíčové slovo „CHARLES“. Vytvoříme tabulku 5 x 5 pro 25 písmen. Protože abeceda má 26 písmen, vynecháme např. písmeno „Q“, které se v českém textu nevyskytuje. Doplníme abecedu do tabulky:

| | | | | |
|---|---|---|---|---|
| **C** | **H** | **A** | **R** | **L** |
| **E** | **S** | B | D | F |
| G | I | J | K | M |
| N | O | P | T | U |
| V | W | X | Y | Z |

Nejprve rozdělíme text na digramy. Pokud se v digramu objeví dvě stejná písmena, vkládá se mezi ně např. dvojice písmen „X“, „Y“. Jestliže je počet písmen lichý, poslední digram se doplní např. písmenem „X“.

Rozdělení otevřeného textu na digramy:

Slunce hezky hřeje. SL UN CE HE ZK YH RE JE (Sudý počet písmen.)

Měsíc pěkně svítí. ME SI CP EK NE SV IT I**X** (Lichý počet – přidat „X“ na konec textu.)

Karel lekl lopaty. KA RE **LX YL** EK **LX YL** OP AT YX.
(Dvě písmena v digramu stejná, vkládá se **XY**.)

Šifrování digramů:

1. část

| | | | | |
|---|---|---|---|---|
| C | H | A | R | L |
| **E** | S | B | **D** | F |
| **G** | **I** | J | K | **M** |
| N | **O** | **P** | T | U |
| V | W | X | **Y** | Z |

| Otevřený: | Šifrovaný: |
|---|---|
| **PO** | **TP** |
| **IM** | **JG** |
| **EG** | **GN** |
| **DY** | **KR** |

2. část

| | | | | |
|---|---|---|---|---|
| C | H | A | R | L |
| E | **S** | B | **D** | F |
| G | I | J | K | M |
| N | **O** | P | **T** | U |
| V | W | X | Y | Z |

| Otevřený: | Šifrovaný: |
|---|---|
| **DO** | **ST** |

| | | | | |
|---|---|---|---|---|
| **C** | H | **A** | R | L |
| E | S | B | D | F |
| G | I | J | K | M |
| **N** | O | **P** | T | U |
| V | W | X | Y | Z |

| Otevřený: | Šifrovaný: |
|---|---|
| **NA** | **PC** |

Ukázka šifrovaného textu:

Měsíc pěkně svítí.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ME | SI | CP | EK | NE | SV | IT | IX |
| GF | IO | AN | DG | VG | EW | KO | JW |

Při dešifrování postupujeme obráceně.

# ŠIFROVÁNÍ – PRACOVNÍ LIST

## Zadání úloh:

Úloha č. 1:
Pracujte s Caesarovou šifrou

Caesarova šifra:

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

Zašifrujte text:

| Text: | n | e | j | s | l | a | v | n | e | j | s | i | o | b | r | a | z | j | e | m | o | n | a | l | i | s | a |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Rozšifrujte text:

| Šifra: | q | h | m | g | h | o | v | l | u | h | n | d | v | y | h | w | d | m | h | d | p | d | c | r | q | n | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Úloha č. 2:
Pracujte s šifrou ATBAŠ:

Šifra ATBAŠ:

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

Zašifrujte text:

| Text: | n | e | j | r | y | c | h | l | e | j | s | i | z | v | i | r | e | n | a | s | o | u | s | i | j | e | g | e | p | a | r | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Rozšifrujte text:

| Šifra: | m | v | q | e | v | g | h | r | a | e | r | i | v | q | v | k | o | v | q | g | e | z | p | l | y | i | l | e | h | p | b |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Úloha č. 3:
Napište tabulku šifry s klíčem „KYTZA“

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

Zašifrujte text:

| Text: | n | e | j | t | v | r | d | s | i | n | e | r | o | s | t | j | e | d | i | a | m | a | n | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | | | | | | | | | | | | | | | | | | | | | | | | |

Rozšifrujte text:

| Šifra: | g | o | k | h | l | s | j | l | r | s | a | z | f | a | i | k | q | a | i | k | q | e | g | k |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | | | | | | | | | | | | | | | | | | | | | | | | |

Úloha č. 4:
Pracujte s POLYALFABETICKOU ŠIFROU – Vigenérova šifra

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

Zašifrujte text s klíčem KRALICEK

| **K** | **R** | **A** | **L** | **I** | **C** | **E** | **K** | K | R | A | L | I | C | E | K | K | R | A | L | I | C | E | K | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | E | J | V | Y | S | S | I | H | O | R | A | J | E | M | O | N | T | E | V | E | R | E | S | T |
| | | | | | | | | | | | | | | | | | | | | | | | | |

Rozšifrujte text s klíčem KRALICEK

| K | R | A | L | I | C | E | K | K | R | A | L | I | C | E | K | K | R | A | L | I | C | E | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | V | J | G | G | U | W | S | R | F | R | L | K | G | G | R | T | V | S | Y | M | B | O | K |
| | | | | | | | | | | | | | | | | | | | | | | | |

Úloha č. 5:
Pracujte s POLYGRAMOVOU ŠIFROU – Playfairova šifra

Zašifrujte a odšifrujte text s klíčem ZAJICEK

Šifrovací čtverec:

| Z | A | J | I | C |
|---|---|---|---|---|
| E | K | | | |
| | | | | |
| | | | | |
| | | | | |

Otevřený text: Pavel lezl loukou do kopce.

Rozdělení na digramy:

Zašifrovaný text:

Odšifrujte:

| s | c | | p | c | | m | c | | f | t | | j | p | | j | a | | j | m | | h | c | | g | b | | e | s | | u | p | | v | e | | o | w |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

# Řešení úloh:

Úloha č. 1:

Pracujte s Caesarovou šifrou

Caesarova šifra:

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

Zašifrujte text:

| Text: | n | e | j | s | l | a | v | n | e | j | s | i | o | b | r | a | z | j | e | m | o | n | a | l | i | s | a |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | q | h | m | v | o | d | y | q | h | m | v | l | r | e | u | d | c | m | h | p | r | q | d | o | l | v | d |

Rozšifrujte text:

| Šifra: | q | h | m | g | h | o | v | l | u | h | n | d | v | y | h | w | d | m | h | d | p | d | c | r | q | n | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | n | e | j | d | e | l | s | i | r | e | k | a | s | v | e | t | a | j | e | a | m | a | z | o | n | k | a |

Úloha č. 2:

Pracujte s šifrou ATBAŠ:

Šifra ATBAŠ:

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

Zašifrujte text:

| Text: | n | e | j | r | y | c | h | l | e | j | s | i | z | v | i | r | e | n | a | s | o | u | s | i | j | e | g | e | p | a | r | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | m | v | q | i | b | x | s | o | v | q | h | r | a | e | r | i | v | m | z | h | l | f | h | r | q | v | t | v | k | z | i | w |

Rozšifrujte text:

| Šifra: | m | v | q | e | v | g | h | r | a | e | r | i | v | q | v | k | o | v | q | g | e | z | p | l | y | i | l | e | h | p | b |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | n | e | j | v | e | t | s | i | z | v | i | r | e | j | e | p | l | e | j | t | v | a | k | o | b | r | o | v | s | k | y |

Úloha č. 3:
Napište tabulku šifry s klíčem „KYTZA“

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

Zašifrujte text:

| Text: | n | e | j | t | v | d | s | i | n | e | r | o | s | t | j | e | d | i | a | m | a | n | t |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Šifra: | j | a | f | q | s | z | p | e | j | a | o | l | p | q | f | a | z | e | k | i | k | j | q |

Rozšifrujte text:

| Šifra: | g | o | k | h | l | s | j | l | r | s | a | z | f | a | i | k | q | a | i | k | q | e | g | k |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Překlad: | k | r | a | l | o | v | n | o | u | v | e | d | j | e | m | a | t | e | m | a | t | i | k | a |

Úloha č. 4:
Pracujte s POLYALFABETICKOU ŠIFROU – Vigenérova šifra

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

Zašifrujte text s klíčem KRALICEK

| **K** | **R** | **A** | **L** | **I** | **C** | **E** | **K** | K | R | A | L | I | C | E | K | K | R | A | L | I | C | E | K | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | E | J | V | Y | S | S | I | H | O | R | A | J | E | M | O | N | T | E | V | E | R | E | S | T |
| X | V | J | G | G | U | W | S | R | F | R | L | R | G | Q | Y | X | K | E | G | M | T | I | C | D |

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **K** | **R** | **A** | **L** | **I** | **C** | **E** | **K** | K | R | A | L | I | C | E | K | K | R | A | L | I | C | E | K |
| X | V | J | G | G | U | W | S | R | F | R | L | K | G | G | R | T | V | S | Y | M | B | O | K |
| N | E | J | V | Y | S | S | I | H | O | R | A | C | E | C | H | J | E | S | N | E | Z | K | A |

Úloha č. 5:

Pracujte s POLYGRAMOVOU ŠIFROU – Playfairova šifra

Zašifrujte a odšifrujte text s klíčem ZAJICEK

Šifrovací čtverec:

| | | | | |
|---|---|---|---|---|
| **Z** | **A** | **J** | **I** | **C** |
| **E** | **K** | B | D | F |
| G | H | L | M | N |
| O | P | R | S | T |
| U | V | W | X | Y |

Otevřený text: Pavel lezl loukou do kopce.

Rozdělení na digramy:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p | a | | v | e | | l | x | | y | l | | e | z | | l | x | | y | l | | o | u | | k | o | | u | d | | o | k | | o | p | | c | e |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Zašifrovaný text:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p | a | | v | e | | l | x | | y | l | | e | z | | l | x | | y | l | | o | u | | k | o | | u | d | | o | k | | o | p | | c | e |
| v | k | | u | k | | m | w | | w | n | | g | e | | m | w | | w | n | | u | z | | e | p | | x | e | | p | e | | p | r | | z | f |

Odšifrujte:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| s | c | | p | c | | m | c | | f | t | | j | p | | j | a | | j | m | | h | c | | g | b | | e | s | | u | p | | v | e | | o | w |
| t | i | | t | a | | n | i | | c | n | | a | r | | a | z | | i | l | | n | a | | l | e | | d | o | | v | o | | u | k | | r | u |

Interreg
EVROPSKÁ UNIE
Rakousko-Česká republika
Evropský fond pro regionální rozvoj

## Příloha:

Tabula recta – Vigenérova šifra – možnost nakopírovat žákům pro snadnější orientaci

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

# ŠIFROVÁNÍ – REFERENCE

[1] Mendelova univerzita v Brně, https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7023

[2] Michal Musílek, Univerzita HK, http://musilek.eu/michal/sifry

[3] Wikipedie:
https://cs.wikipedia.org/wiki/Homofonn%C3%AD_%C5%A1ifrahttps://sk.wikipedia.org/wiki/Atba%C5%A1
[4] Wikipedie:
https://cs.wikipedia.org/wiki/Vigen%C3%A8rova_%C5%A1ifra
[5] Wikipedia:
https://sk.wikipedia.org/wiki/Kryptol%C3%B3gia