Program pro (de)šifrování xor šifry

Jan Bezouška

3.A

Obsah

[1. Úvod 2](#_Toc66711392)

[2. XOR Šifra 2](#_Toc66711393)

[3. Program 2](#_Toc66711394)

[3.1 Postup 2](#_Toc66711395)

[4. Závěr 2](#_Toc66711396)

# Úvod

Tento document popisuje mnou vytvořený program, a šifru, kterou program využívá.

*Program ke stažení, a popsaný zdrojový kód, je k nalezení zde: github.com/janbezouska/XOR\_Cipher*

# XOR Šifra

Jedná se o jednoduchou aditivní šifru.

Funguje na následujícím principu, ve kterém ⊕ značí exkluzivní disjunkci (XOR):

A ⊕ 0 = A,

A ⊕ A = 0,

A ⊕ B = B ⊕ A,

(A ⊕ B) ⊕ C = A ⊕ (B ⊕ C),

(B ⊕ A) ⊕ A = B ⊕ 0 = B.[[1]](#footnote-1)

Šifrování i dešifrování funguje stejně, a to tak, že se nejdříve převede znak textu a klíče na 8-bitovou ascii hodnotu. Poté se mezi těmito hodnotami provede exkluzivní disjunkce. Tento proces pokračuje do té doby, dokud nejsou od/zašifrovány všechny znaky textu.

# Program

Program je vytvořen pomocí Windows Presentation Foundation(WPF). Skládá se z následujících prvků:

* 2x tlačítko – šifrování; dešifrování
* 2x RichTextBox – zadání textu pro šifrování + vypsání dešifrovaného textu; zadání textu pro dešifrování + vypsání zašaifrovaného textu
* 2x TextBox – zadání klíče; vypsání chyb
* 3x Label – popisy jiných prvků

# Postup

Nejprve jsem vytvořil jednotlivé prvky pomocí xamlu, a tlačítkům jsem přiřadil eventy. Poté jsem vytvořil metodu, ve které se provádí (de)šifrování. V té jsem nejdříve naprogramoval ohlídání, a případné vypsání, chyb. Následně stačilo napsat samotné (de)šifrování, a vypsání výsledného textu, což je v případě XOR šifry vcelku jednoduché.Závěr

# Závěr

Díky tomuto projektu jsem se dozvěděl více o XOR šifře, a hlavně jsem se blíže seznámil s WPF a xaml, se kterým právě začínáme v programování.

1. XOR Cipher. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-03-15]. Dostupné z: https://en.wikipedia.org/wiki/XOR\_cipher [↑](#footnote-ref-1)