FAKULTA STROJNÍHO INŽENÝRSTVÍ ústav automatizace a informatiky

Caesarova šifra

19. 12. 2023

David Bystroň, 228676

David Bystroň, 228676

Caesarova šifra

Caesarova šifra je jedna z nejjednodušších šifer, pojmenovaná po Gaiu Juliu Caesarovi, který ji používal na šifrování vojenských zpráv.

Jedná se o substituční šifru. To znamená, že jednotlivá písmena v otevřeném textu jsou nahrazena jinými písmeny podle daného klíče. Konkrétně v této šifře je klíčem číslo, které určuje o kolik pozic posuneme danou abecedu. Například pokud by byl klíč číslo 2, písmeno A by bylo nahrazeno písmenem C, B za D atd.

Prolomení šifry není nikterak složité, jelikož počet možných klíčů je dán velikostí použité abecedy. Je tak náchylná na použití "hrubé síly" k dešifrování.

Frekvenční kryptoanalýza

Frekvenční analýza je jednoduše počítání písmen, nebo skupin písmen v šifrovaném textu. Vychází ze skutečnosti, že určitá písmena se v textu vyskytují s různou četností.

Každý jazyk má pak charakteristické rozložení jednotlivých znaků. Například v angličtině se nejčastěji vyskytuje písmeno E, pak písmeno T. Písmena jako Z nebo X se pak vyskytují s velmi malou četností.

Tohoto faktu pak můžeme využít k prolomení Caesarovy šifry, kde spočítáme frekvence jednotlivých znaků a porovnáme je se známými frekvencemi písmen určitého jazyka.

V samotném kódu pak byly použity tyto frekvenční rozložení znaků:

```
english_letter_frequencies = {' ': 20, 'A': 8.17, 'B': 1.49, 'C': 2.78, 'D': 4.25, 'E': 12.70, 'F': 2.23,
                              'G': 2.02, 'H': 6.09, 'I': 6.97, 'J': 0.15, 'K': 0.77, 'L': 4.03, 'M': 2.41,
                              'N': 6.75, 'O': 7.51, 'P': 1.93, 'Q': 0.10, 'R': 5.99, 'S': 6.33, 'T': 9.06,
                              'U': 2.76, 'V': 0.98, 'W': 2.36, 'X': 0.15, 'Y': 1.97, 'Z': 0.07}


czech_letter_frequencies = {' ': 20, 'A': 8.35, 'B': 1.23, 'C': 4.41, 'D': 3.99, 'E': 9.21, 'F': 0.82,
                            'G': 1.52, 'H': 1.46, 'I': 6.94, 'J': 2.17, 'K': 3.73, 'L': 3.54, 'M': 3.15,
                            'N': 6.83, 'O': 6.26, 'P': 2.42, 'Q': 0.01, 'R': 5.87, 'S': 6.02, 'T': 5.05,
                            'U': 3.41, 'V': 5.23, 'W': 0.02, 'X': 0.03, 'Y': 4.74, 'Z': 4.64}
```

Dešifrování pak probíhá tak, že vyzkoušíme všechny možné posunutí šifrovaného textu a pro každý klíč spočítáme podobnost s angličtinou, případně češtinou. Nejvyšší podobnost s daným jazykem má pak samozřejmě originální zpráva.

David Bystroň, 228676

Uživatelský popis programu

Celý kód lze ovládat pouze pomocí terminálu. Uživatel si nejprve vybere, zda chce svou zprávu enkódovat nebo dekódovat, případně jestli chce program ukončit.

V šifrovaném i otevřeném textu jsou povoleny pouze znaky anglické abecedy a mezera.

Pokud budeme chtít zprávu zakódovat, program nás nejprve vyzve k zadání zprávy a poté k zadání klíče, ten musí mít hodnotu celého čísla. Poté se zobrazí šifrovaná zpráva.

Type 'en' to encode the message, 'de' to decode the message or 'end' for end program:

en

Enter the message:

Prisel jsem videl jsem zvitezil jsem

Enter the key:

4

Your encrypt message is: TVMWIPDNWIQDZMHIPDNWIQDCZMXICMPDNWIQ

V případě, že chceme zprávu dekódovat, musíme nejprve zvolit jazyk ve kterém je text psán. To je z důvodu různých četností písmen v jednotlivých jazycích. Poté už jen vložíme šifru a program nám zobrazí původní zprávu.

Type 'en' to encode the message, 'de' to decode the message or 'end' for end program:

de

Type 'CZ' or 'EN' for choosing language:

cz

Enter the message:

TVMWIPDNWIQDZMHIPDNWIQDCZMXICMPDNWIQ

Original message is: PRISEL JSEM VIDEL JSEM ZVITEZIL JSEM

Zdroje

Caesar cipher. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://en.wikipedia.org/wiki/Caesar_cipher. [cit. 2023-12-21].

Frequency analysis. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://en.wikipedia.org/wiki/Frequency_analysis. [cit. 2023-12-21].

Crack the Code: The Caesar Cipher [@Paget Teaches]. Online. Dostupné z: YouTube, https://www.youtube.com/watch?v=UkTHgQ_qwJk. [cit. 2023-12-21].