

Szyfr Homofoniczny

Podstawieniowy z kluczem

Krzysztof Świdorski (272313), Cyberbezpieczeństwo

Opis

Homophonic_substitution_cipher_v1 to program napisany w języku Python. Ściślej mówiąc, jest to implementacja szyfru homofonicznego podstawieniowego z tajnym kluczem. Program pozwala użytkownikowi na zaszyfrowanie prostych tekstowych wiadomości wspomnianym szyfrem, odszyfrowanie ich oraz wygenerowanie klucza, który jest niezbędny do poprawnego zaszyfrowania oraz odczytania tajnej wiadomości. Klucz jest zapisywany w formie pliku, w folderze gdzie znajduje się program.

Projekt składa się z głównego pliku

Homophonic_substitution_cipher_v1.py oraz pliku uruchamiającego **run.py**.

Pojęcia:

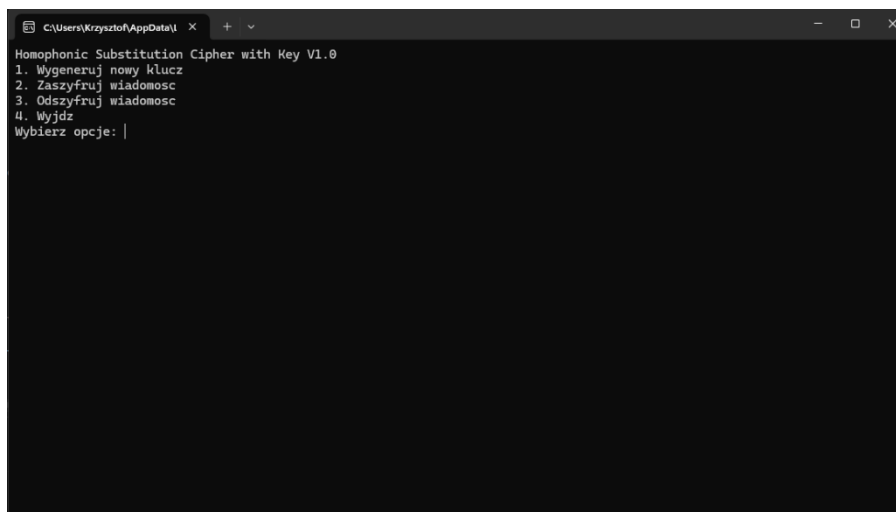
Szyfr podstawieniowy – szyfrowanie polegające na zastąpieniu każdego znaku tekstu jawnego innym znakiem. Np. A – 30, B – 46, C – 89 itd.

Szyfr homofoniczny – rodzaj szyfru podstawieniowego, w którym każdej literze tekstu jawnego odpowiada inny zbiór symboli (homofonów). Np. A = {4, 56, 96} – litera 'A' może być zaszyfrowana jako 4, 56 lub 96.

Tajny klucz – w kontekście tego programu kluczem jest lista wszystkich możliwych znaków i przypisane im wartości liczbowe. Na podstawie klucza szyfrowane i odszyfrowywane są wiadomości.

Wymagania:

Zainstalowany Python (preferowana wersja 3.10)



Działanie oraz instrukcja:

Pliki **Homophonic_substitution_cipher_v1.py** oraz **run.py** należy umieścić w wybranym przez nas folderze.

Po uruchomieniu programu **run.py**, w pierwszej kolejności wyświetla się menu główne. Użytkownik ma do wyboru:

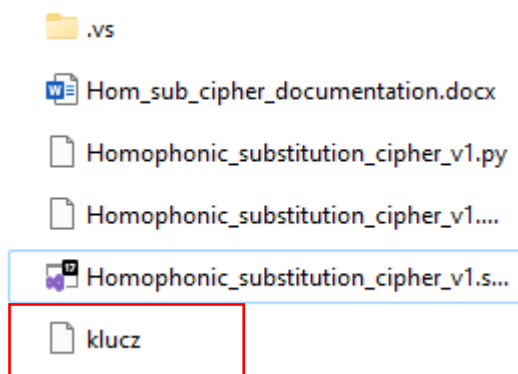
- Wygenerować unikalny klucz i zapisać go w folderze, w którym znajduje się program
- Zaszzyfrować wiadomość wygenerowanym kluczem
- Odszyfrować wiadomość kluczem
- Zakończyć działanie programu

Wybór dokonywany jest poprzez wpisanie odpowiedniej cyfry i naciśnięcie ENTER.

W pierwszej kolejności należy wygenerować klucz, który jest niezbędny do zaszzyfrowania i odszyfrowania wiadomości.

```
C:\Users\Krzysztof\AppData\Local\Microsoft\WindowsApps\PythonSoftwareFoundation.Python.3.9_...
Homophonic Substitution Cipher with Key V1.0
1. Wygeneruj nowy klucz
2. Zaszzyfruj wiadomosc
3. Odszyfruj wiadomosc
4. Wyjdz
Wybierz opcje: 1
Podaj nazwe klucza, aby zapisac go jako plik: klucz
```

W tym momencie klucz został zapisany jako plik.



```
Plik  Edytuj  Wyświetl  [Settings Icon]
[{"A": [675, 102, 611], "B": [947, 135, 449], "C": [519, 453, 472], "D": [393, 613, 595], "E": [869, 544, 468], "F": [288, 990, 901], "G": [470, 336, 124], "H": [587, 186, 840], "I": [543, 758, 127], "J": [591, 445, 688], "K": [405, 686, 717], "L": [540, 235, 715], "M": [328, 747, 640], "N": [925, 908, 982], "O": [776, 952, 297], "P": [385, 849, 152], "Q": [146, 345, 417], "R": [487, 194, 668], "S": [144, 634, 479], "T": [142, 528, 916], "U": [161, 755, 374], "V": [388, 969, 342], "W": [948, 181, 958], "X": [507, 864, 770], "Y": [963, 946, 281], "Z": [329, 294, 354]}
```

Szyfrowanie

Teraz zaszyfrujemy prostą wiadomość: Spotkajmy się jutro w parku, o tej godzinie co zwykle.

Dla poprawnego działania usuwamy najpierw polskie znaki oraz znaki interpunkcyjne: Spotkajmy sie jutro w parku o tej godzinie co zwykle

Wybieramy odpowiednią opcję i podajemy nazwę klucza.

```
C:\Users\Krzysztof\AppData\Local\Microsoft\Windows\Terminal\1
Homophonic Substitution Cipher with Key V1.0
1. Wygeneruj nowy klucz
2. Zaszzyfruj wiadomosc
3. Odszyfruj wiadomosc
4. Wyjdz
Wybierz opcje: 2
Podaj nazwe pliku (klucza): klucz
Podaj wiadomosc do zaszzyfrowania: Spotkajmy sie jutro w parku o tej godzinie co zwykle
Zaszzyfrowana wiadomosc: 479 152 776 528 686 675 445 640 963 144 758 544 591 161 142 487 952 181 385 675 668 405 755 776
142 544 445 336 952 613 294 758 908 127 468 453 297 329 958 946 686 235 544
Homophonic Substitution Cipher with Key V1.0
1. Wygeneruj nowy klucz
2. Zaszzyfruj wiadomosc
3. Odszyfruj wiadomosc
4. Wyjdz
Wybierz opcje: |
```

Otrzymujemy ciąg liczb – szyfrogram. Jak można zauważyć, białe znaki są pomijane podczas szyfrowania i dzięki temu nie możemy stwierdzić gdzie kończą się słowa oraz z ilu składa się wiadomość. Każdej literze przyporządkowana jest jedna z trzech losowych liczb 3 cyfrowych.

Odszyfrowanie

```
C:\Users\Krzysztof\AppData\Local\Microsoft\Windows\Terminal\1
Homophonic Substitution Cipher with Key V1.0
1. Wygeneruj nowy klucz
2. Zaszzyfruj wiadomosc
3. Odszyfruj wiadomosc
4. Wyjdz
Wybierz opcje: 3
Podaj nazwe pliku (klucza): klucz
Podaj zaszzyfrowany tekst: 479 152 776 528 686 675 445 640 963 144 758 544 591 161 142 487 952 181 385 675 668 405 755 776
6 142 544 445 336 952 613 294 758 908 127 468 453 297 329 958 946 686 235 544
Odszyfrowana wiadomosc: SPOTKAJMYSIEJUTROWPARKUOTEJGODZINIECOZWYKLE
Homophonic Substitution Cipher with Key V1.0
1. Wygeneruj nowy klucz
2. Zaszzyfruj wiadomosc
3. Odszyfruj wiadomosc
4. Wyjdz
Wybierz opcje:
```

Proces odszyfrowywania wygląda bardzo podobnie – musimy podać nazwę klucza oraz zaszyfrowaną wiadomość. Ważne jest żeby podać szyfrogram **z białymi znakami**, w takiej formie jak po zaszyfrowaniu. Nie należy łączyć liczb w jeden długi ciąg.

Program umożliwia wygenerowanie wielu kluczy, więc jeśli jeden zostanie skompromitowany, to informacje mogą zostać szybko zaszyfrowane drugim.