Raport Szyfr Cezara

Tomasz Śmiech ; Rafał Kolaska

08.02.2019

1 Wstęp

W celu zaliczenia przedmiotu przygotowaliśmy prezentację na temat Szyfru Cezara, który zaimplementowaliśmy w języku haskell.

2 O szyfrze

Jest to jeden z najprostszych szyfrów podstawieniowych, w którym litery w tekście pierwotnym są zastępowane literami oddalonymi o zadaną wcześniej liczbę pozycji w danym alfabecie. Nazwa szyfru pochodzi od Juliusza Cezara, który używał szyfru w listach do swoich przyjaciół.

3 Matematyka

Zagadnienie można wyrazić za pomocą arytmetyki modularnej.
Każdej literze w alfabecie przyporządkujemy liczbę:
A− >0, B− >1, ..., Z− >24 (Alfabet Łaciński)
n-liczba z zakresu $0 - 24$ (numer zaszyfrowanej litery A)
$Z(x)_n x + n$
$Z(x)_n$ - numer zaszyfrowanej litery,
x - numer litery do zaszyfrowania

$Y(y)_n y - n$
$Y(y)_n$ - numer odszyfrownej litery,
x - numer litery zaszyfrowanej Jeśli przy wyznaczaniu $Z(x)_n$ wartość wyrażenia $x + n$ przekroczy 23 , to należy ją zmniejszyć o 24.

Jeśli przy wyznaczaniu $Y(y)_n$ wartość wyrażenia y n będzie ujemna, to należy ją zwiększyć o 24.

4 Źródła

`https://pl.wikipedia.org/wiki/Szyfr_Cezara`