

Algorytmy i struktury danych

Sprawozdanie z Zadania nr: 6

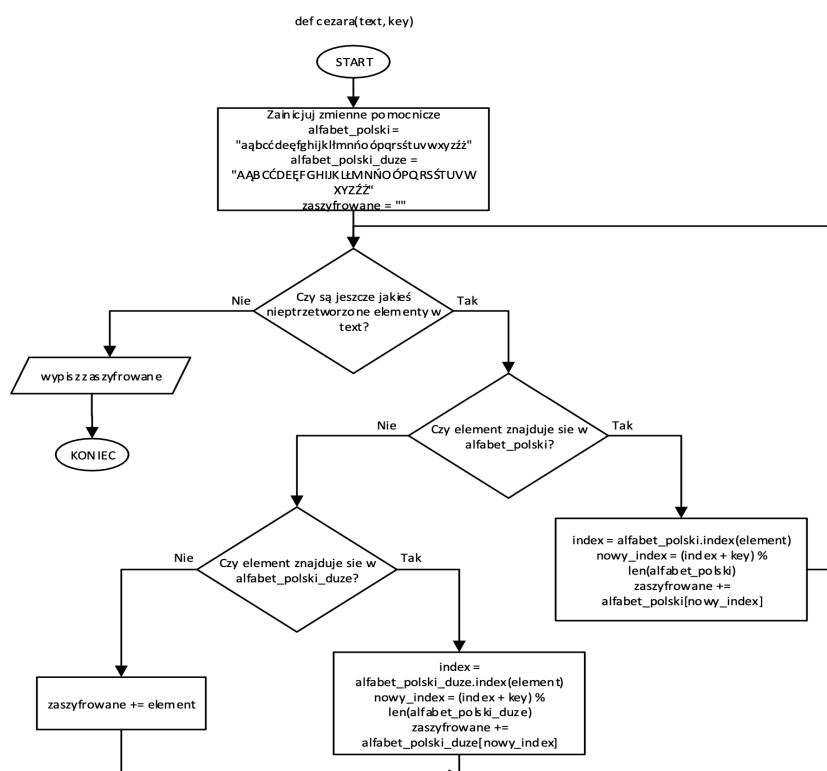
Imię i Nazwisko: Bartosz Ochnik

Data: 09.12.2024r

Cezara z dowolnym przesunięciem

Opis teoretyczny: Szyfr Cezara to prosty algorytm szyfrowania tekstu, polegający na przesunięciu każdej litery w alfabecie o stałą liczbę miejsc. Na przykład, przy przesunięciu o 3, litera „A” staje się „D”. Szyfr działa na zasadzie przekształcenia każdej litery zgodnie z ustaloną regułą (modulo liczba liter w alfabecie). Jego prostota czyni go podatnym na ataki kryptoanalityczne, ale w prostych zastosowaniach może być wystarczający. Jest to przykład szyfru podstawieniowego.

Opis schematem blokowym:



Przykłady wykorzystania:

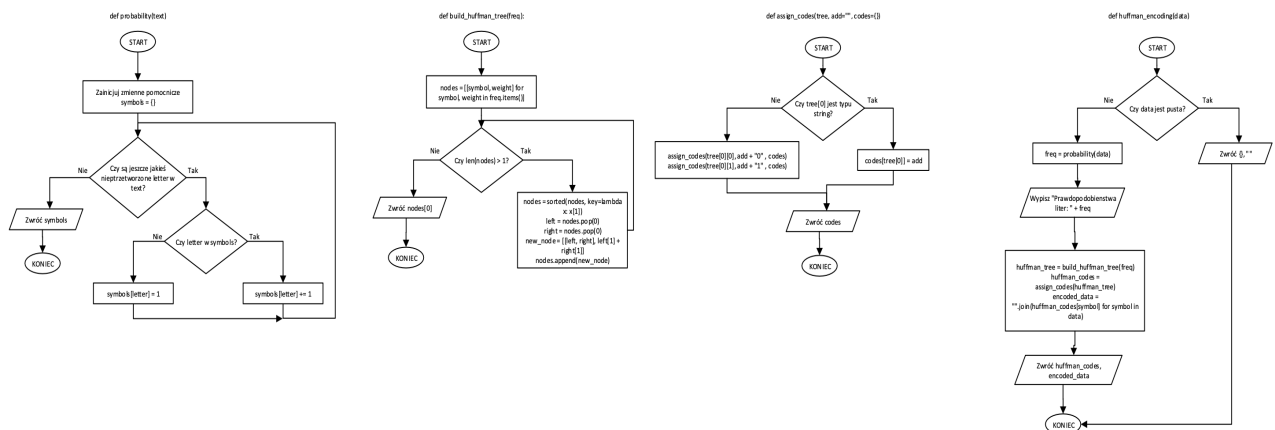
- **Podstawowe zabezpieczenie danych:** Szyfr Cezara może być używany do zabezpieczania mało ważnych danych w systemach, gdzie nie jest wymagana wysoka poufność.
- **Nauka kryptografii:** Dzięki prostocie algorytmu jest on często wykorzystywany w edukacji do wprowadzenia podstawowych pojęć kryptograficznych.
- **Zabawy i gry:** W grach komputerowych lub escape roomach szyfr Cezara bywa stosowany jako element zagadek logicznych.

Algorytmy i struktury danych

Huffmana

Opis teoretyczny: Algorytm Huffmana to optymalna metoda kodowania bezstratnego, która minimalizuje średnią długość kodu dla danego zestawu symboli na podstawie ich częstości występowania. Wykorzystuje drzewo binarne, w którym symbole o najwyższej częstości mają krótsze kody, a rzadsze symbole – dłuższe. Proces budowy kodu polega na iteracyjnym łączeniu dwóch symboli o najniższych prawdopodobieństwach i przypisywaniu im wspólnego węzła, aż powstanie pełne drzewo. Algorytm jest szeroko stosowany w kompresji danych.

Opis schematem blokowym:



Przykłady wykorzystania:

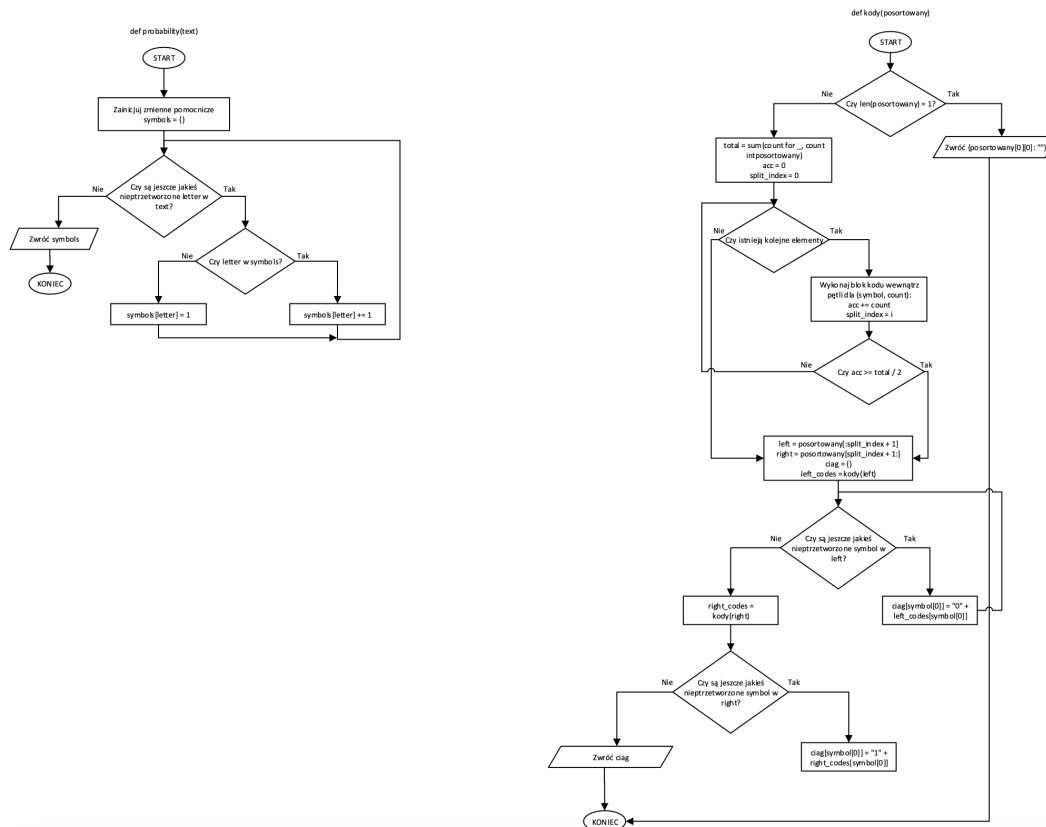
- **Kompresja plików:** Algorytm Huffmana jest wykorzystywany w formatach takich jak ZIP czy JPEG do redukcji rozmiaru plików.
- **Kodowanie transmisji danych:** W telekomunikacji i transmisji strumieniowej stosuje się go do optymalizacji przepustowości, minimalizując liczbę przesyłanych bitów.
- **Kompresja tekstu:** Służy do efektywnej reprezentacji tekstu w formatach takich jak archiwa TAR.GZ lub w implementacjach kompresji JSON/XML.

Algorytmy i struktury danych

Shannona-Fano

Opis teoretyczny: Algorytm Shannona-Fano służy do kodowania danych w sposób minimalizujący ich długość, opierając się na prawdopodobieństwie występowania symboli. Znaki o wyższym prawdopodobieństwie są kodowane krótszymi ciągami bitów, a znaki rzadsze – dłuższymi. Algorytm dzieli symbole na grupy w taki sposób, aby suma ich prawdopodobieństw była zbliżona. Jest stosowany w kompresji danych, choć został wyparty przez bardziej efektywny algorytm Huffmana.

Opis schematem blokowym:



Przykłady wykorzystania:

- **Kompresja danych:** Algorytm Shannona-Fano znajduje zastosowanie w podstawowych metodach kompresji danych, takich jak kodowanie plików tekstowych.
- **Teoria informacji:** Wykorzystywany jest w nauczaniu podstaw teoretycznych efektywnej reprezentacji informacji.
- **Analiza danych statystycznych:** Może być używany do badania rozkładu prawdopodobieństw symboli w danych, co jest przydatne w procesie optymalizacji formatów danych.