Sprawozdanie z pracowni specjalistycznej

Bezpieczeństwo Sieci Komputerowych

Zajęcia nr 1

Wykonujący ćwicznenie: Marcin Tyborowski i Kacper Świsłocki

Studia dzienne

Kierunek: Informatyka

Semestr: VI

Grupa zajęciowa: PS7

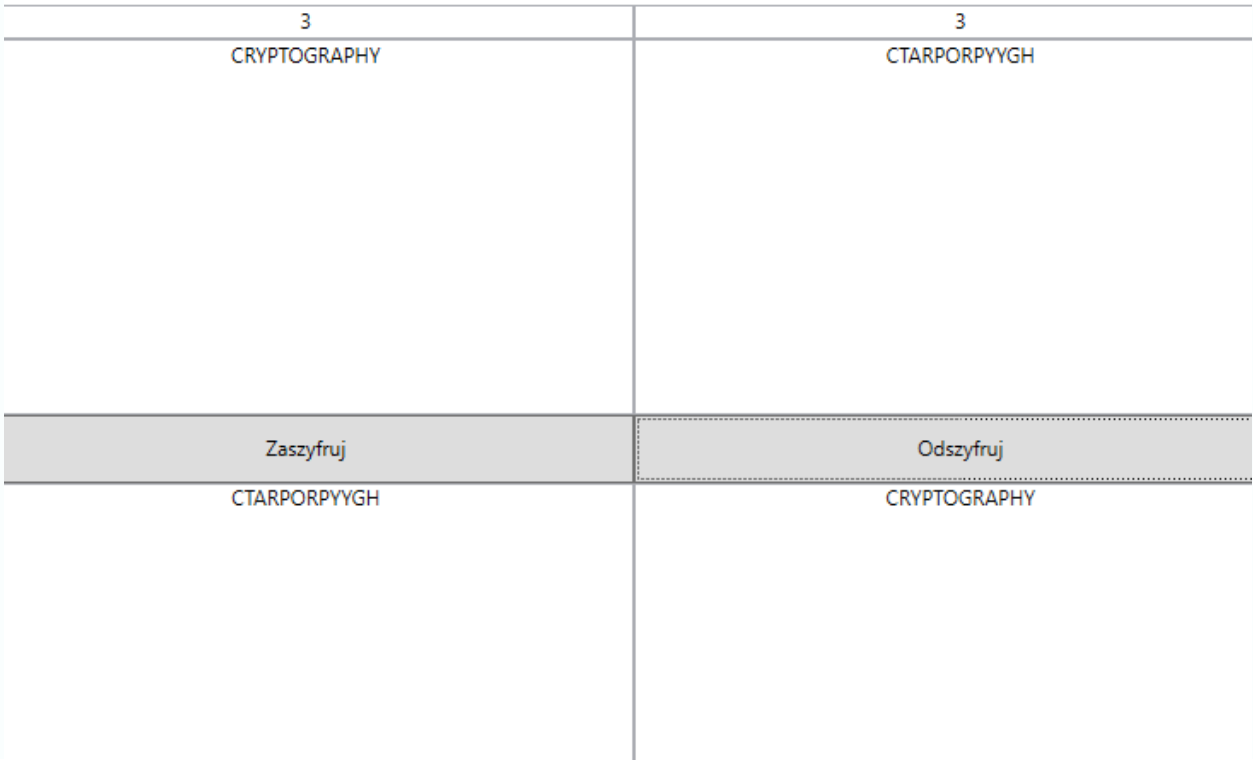
Prowadzący ćwiczenie: mgr inż. Michał Czołombitko

Do wykonania zadań wykorzystano technologię .NET (WPF). Solucja RailFence odpowiada zadaniu pierwszemu, PrzestawieniaMacierzowe drugiemu, PrzestawieniaMacierzowe2 trzeciemu.

Zadanie 1

Zaimplementuj algorytm kodujący i dekodujący z wykorzystaniem szyfru prostego przestawiania *rail fence* dla k = n. Skorzystaj z przykładu 1 (1 punkt).

Aplikacja rozwiązująca zadany problem wygląda następująco:



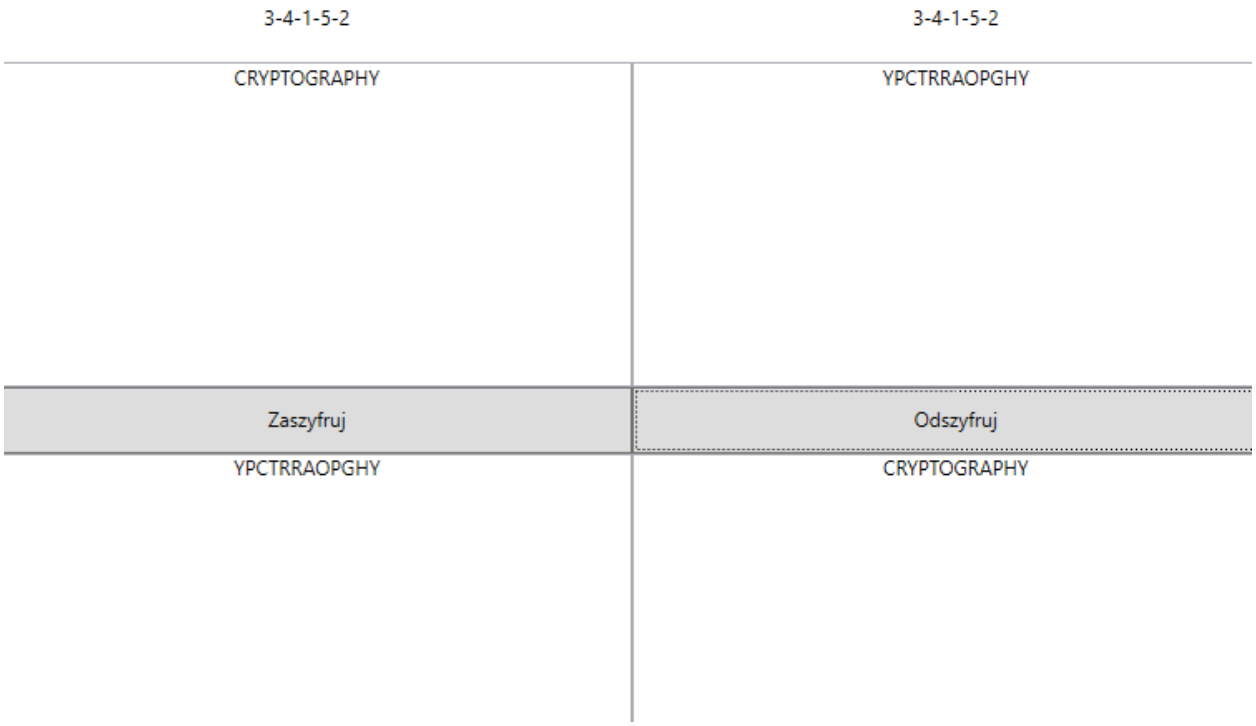
Na górze (w miejscu, gdzie obecnie wpisane jest 3) podaje się wysokość, niżej tekst do zaszyfrowania/odszyfrowania. Po kliknięciu odpowiedniego przycisku na dole pojawi się odpowiedni wynik. **Aby uruchomić aplikację należy uruchomić plik RailFenceWPF.exe.**

Algorytm polega na rozpisywaniu szyfrowanego tekstu w zależności od podanego klucza – wysokości. Następnie tworzone są tak zwane „schodki", w których na zmianę wpisywane są kolejne litery szyfrowanego hasła. Aby odczytać tekst należy odczytywać wartości kolejno od schodków najwyższych do najniższych, od lewej do prawej.

Zadanie 2

Zaimplementuj system kryptograficzny oparty o przestawienie macierzowe pokazane w przykładzie 2a dla d = 5 oraz klucza key = 3-4-1-5-2 (1 punkt).

Aplikacja rozwiązująca zadany problem wygląda następująco:



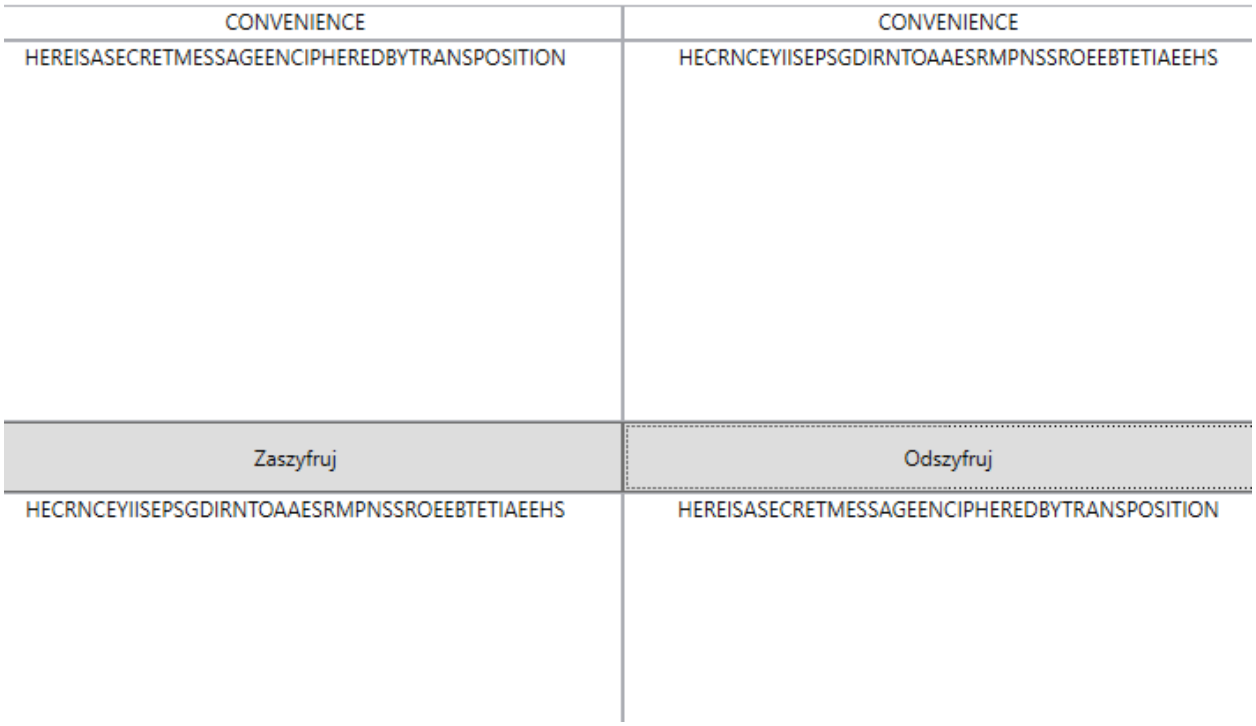
Na samej górze wyświetlany jest klucz, który wstawiony jest na stałe – tak jak nakazano w treści zadania. Można go ewentualnie zmienić w kodzie programu. Pod kluczem podaje się tekst do zaszyfrowania, oraz po kliknięciu odpowiedniego przycisku otrzymywany jest wynik. **Aby uruchomić aplikację należy uruchomić plik PrzestawieniaMacierzowe.exe.**

Algorytm polega na wpisywaniu do macierzy kolejnych liter szyfrowanego hasła według długości zadanego klucza. Następnie należy odczytywać kolejne wiersze tablicy w kolejności zadanej przez klucz.

Zadanie 3

Zaimplementuj system kryptograficzny oparty o przestawienie macierzowe 2b (1 punkt)

Aplikacja rozwiązująca zadany problem wygląda następująco:



Na samej górze wyświetlany jest klucz, który jest polem edytowalnym. Pod kluczem podaje się tekst do zaszyfrowania, oraz po kliknięciu odpowiedniego przycisku otrzymywany jest wynik. **Aby uruchomić aplikację należy uruchomić plik PrzestawieniaMacierzowe2.exe.**

Algorytm polega na wpisywaniu do macierzy kolejnych liter szyfrowanego hasła według długości zadanego klucza. Następnie należy odczytywać kolejne kolumny tablicy (tworzą one słowa zaszyfrowanego tekstu) w kolejności zadanej przez klucz, który jest słowem. Kolejność ustala się na podstawie kolejności liter klucza w alfabecie.