

Politechnika Białostocka Bezpieczeństwo Sieci Komputerowych Grupa PS7	Data przeprowadzenia ćwiczenia: 20.02.2018r. Prowadzący: mgr inż. Michał Czołombitko
Temat: Implementacja podstawowych modułów kryptograficznych Skład zespołu: 1. Kosiński Krzysztof 2. Kwapisz Błażej	Ocena:

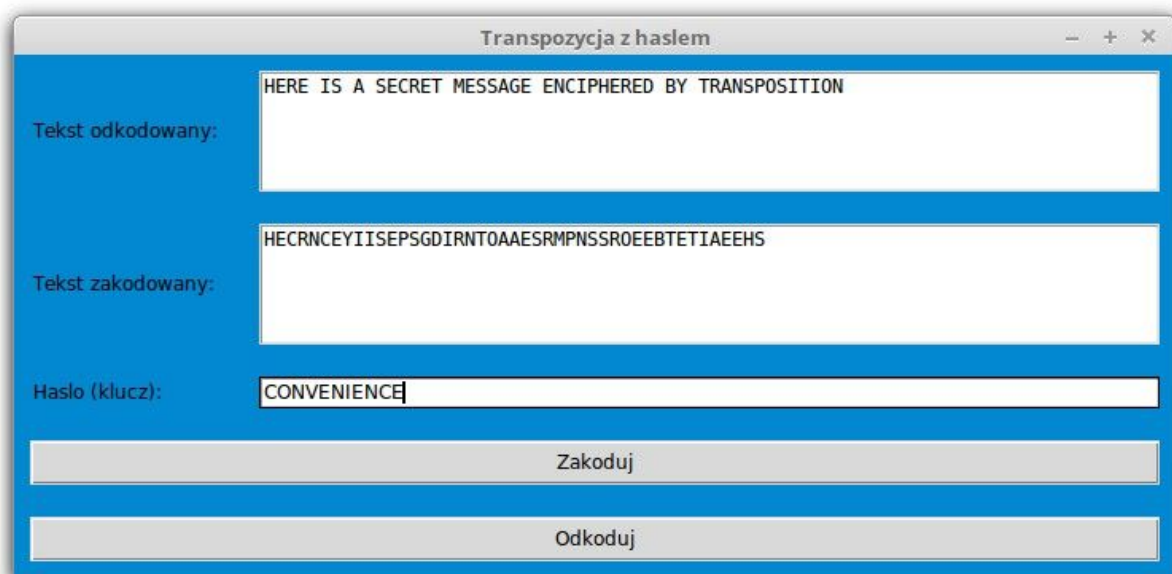
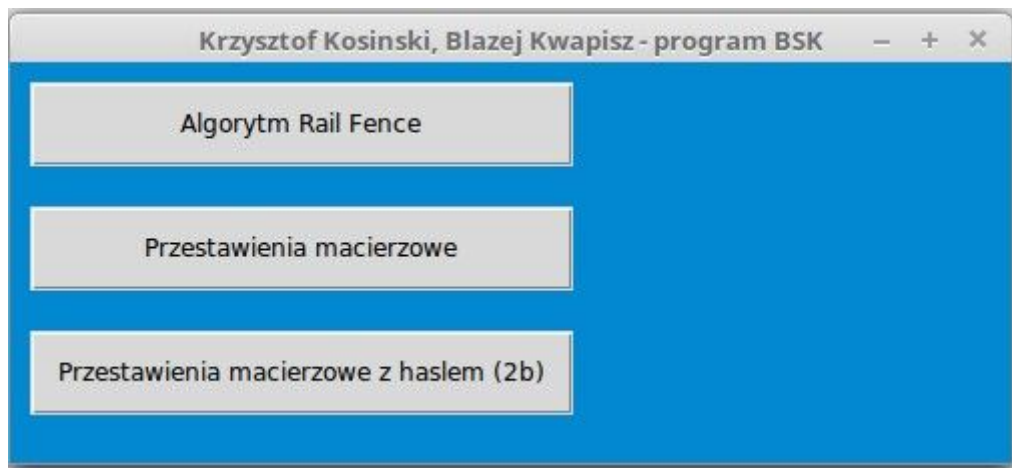
Informacje ogólne

Wykonany został program w języku Python, w którym zrealizowano trzy zadania związane z implementacją podstawowych systemów kryptograficznych: Rail Fence, przestawienie macierzowe oparte o kolejność oraz przestawienie macierzowe oparte o wybrane hasło. Program napisany został z użyciem programowania obiektowego, każdy system kryptograficzny jest oddzielną klasą zawierającą funkcje do szyfrowania i deszyfrowania oraz funkcje pomocnicze. Posiada on podstawowy interfejs graficzny ułatwiający obsługę, zaimplementowany przy użyciu biblioteki TkInter. Dzięki użyciu Pythona, program działa na systemach Windows, Linux i Mac OS X.

Instrukcja obsługi

1. Uruchom program, korzystając z wiersza poleceń poleceniem `./python zad1.py` (lub inne, odpowiednie polecenie do uruchomienia interpretera Pythona na wybranym systemie operacyjnym).
2. Z menu głównego wybierz system kryptograficzny, którego chcesz użyć.
3. Pojawi się menu dla wybranego systemu kryptograficznego. Jeżeli chcesz zakodować wybrany tekst znaków, wpisz (lub wklej) go do okienka "Tekst odkodowany", a następnie naciśnij przycisk Zakoduj. Zakodowany tekst pojawi się w okienku Tekst zakodowany. Jeżeli chcesz odkodować wybrany tekst, wklej lub wpisz go w okienko "Tekst zakodowany", a następnie naciśnij przycisk Odkoduj - odkodowany tekst pojawi się w okienku "Tekst odkodowany". Dla obydwu wypadków, należy przedtem uzupełnić pole "Ilość linii / Wybrany klucz" ilością linii dla algorytmu Rail Fence, bądź też wybranym kluczem szyfrującym dla przestawienia macierzowego.

Zrzuty ekranu programu



Transpozycja z hasłem

Tekst odkodowany:

Tekst zakodowany:

Hasło (klucz):test

Zakoduj

Odkoduj

Błąd

[!] Nie podałeś tekstu do zakodowania.