|  |  |
| --- | --- |
| Bezpieczeństwo Sieci Komputerowych | Data: 16.03.2016r. |
| Autor: **Maciej Sawicki** | Prowadzący:  Dr Inż. Maciej Brzozowski |

Środowisko implementacji ćwiczenia:

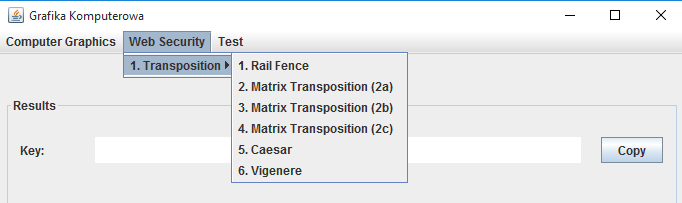
* Java w wersji 1.8.0\_51
* NetBeans IDE w wersji 8.1 (Build 201510222201)
* Windows 10 Educational

Uruchomienie:

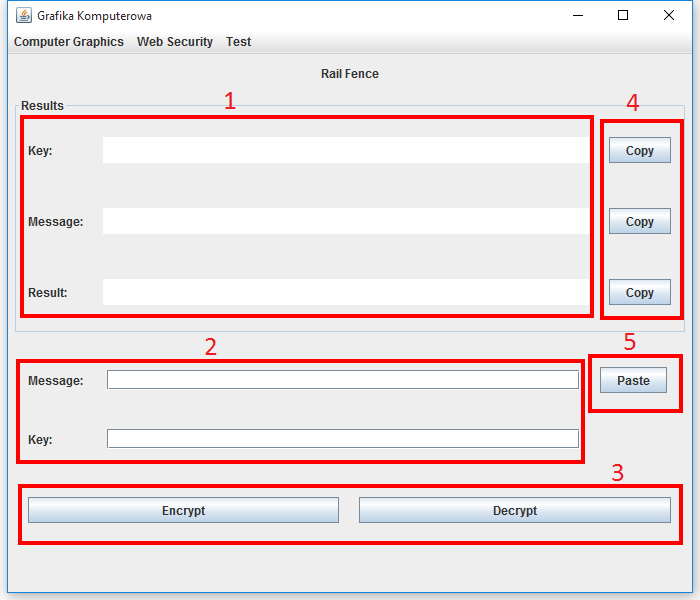
Aby uruchomić program, należy otworzyć plik o nazwie „Grafika Komputerowa.jar” znajdujący się w folderze „bin”.

Wybór algorytmów szyfrujących:

Aby wybrać algorytm szyfrujący należy wejść w zakładkę „Web Security”, następnie w menu „Transposition” i w wybrany algorytm.

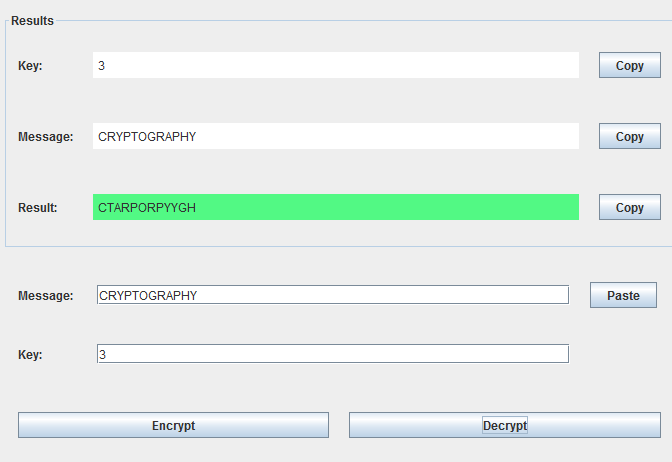


GUI – wyjaśnienie:

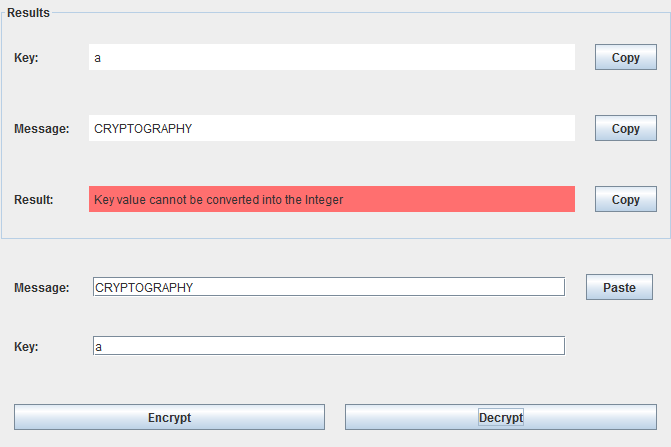


1. Panel, w którym będą wyświetlane wyniki po szyfracji lub deszyfracji.
2. Panel, w którym wpisujemy dane.
3. Panel, w którym wybieramy metodę – szyfrowanie lub deszyfrowanie.
4. Przyciski, które kopiują do schowka systemowego zawartość znajdującą się po ich lewej stronie.
5. Przycisk wklejający zawartość schowka systemowego w miejsce znajdujące się po jego lewej stronie.

Przykład POPRAWNIE wykonanego szyfrowania/deszyfrowania:



Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:

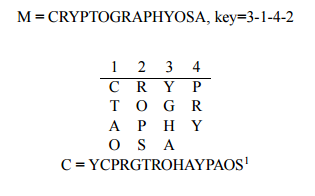


Zad 1 (Rail Fence).

Zaimplementuj algorytm kodujący i dekodujący z wykorzystaniem szyfru prostego przestawienia „Rail Fence” dla k = n.

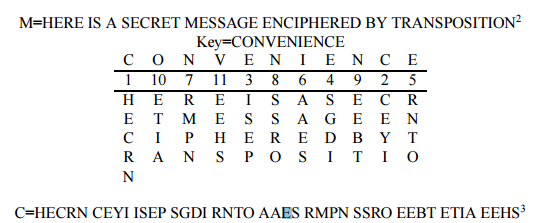
Zad 2 (Matrix Transposition (2a)).

Zaimplementuj kryptosystem przestawieniowy bazujący na podanym przykładzie:

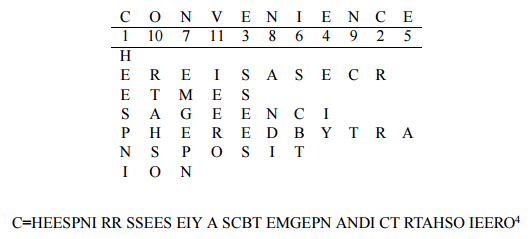


Zad 3.

1. (Matrix Transposition (2b)) Zaimplementuj kryptosystem przestawieniowy bazujący na podanym przykładzie:

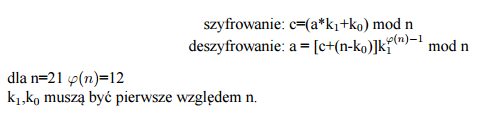


1. (Matrix Transposition (2c)) Zaimplementuj kryptosystem przestawieniowy bazujący na podanym przykładzie:



Zad 4 (Caesar).

Zaimplementuj szyfr cezara bazujący na podanym przykładzie:



Zad 5 (Vigenere).

Zaimplementuj kryptosystem bazujący na tablicy Vigenere’a.