Bezpieczeństwo Sieci Komputerowych	Data: 16.03.2016r.
Ćwiczenie nr 1 Autor: **Maciej Sawicki**	Prowadzący: Dr Inż. Maciej Brzozowski

Środowisko implementacji ćwiczenia:

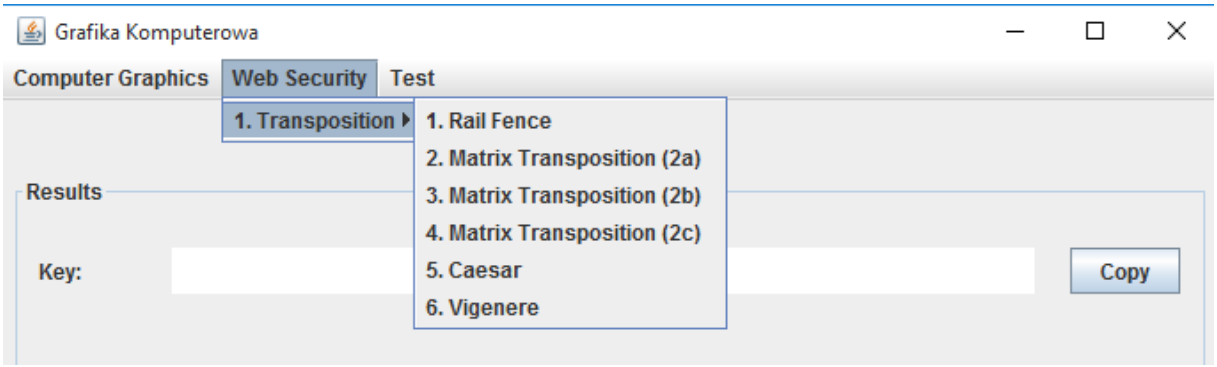
- Java w wersji 1.8.0_51
- NetBeans IDE w wersji 8.1 (Build 201510222201)
- Windows 10 Educational

Uruchomienie:

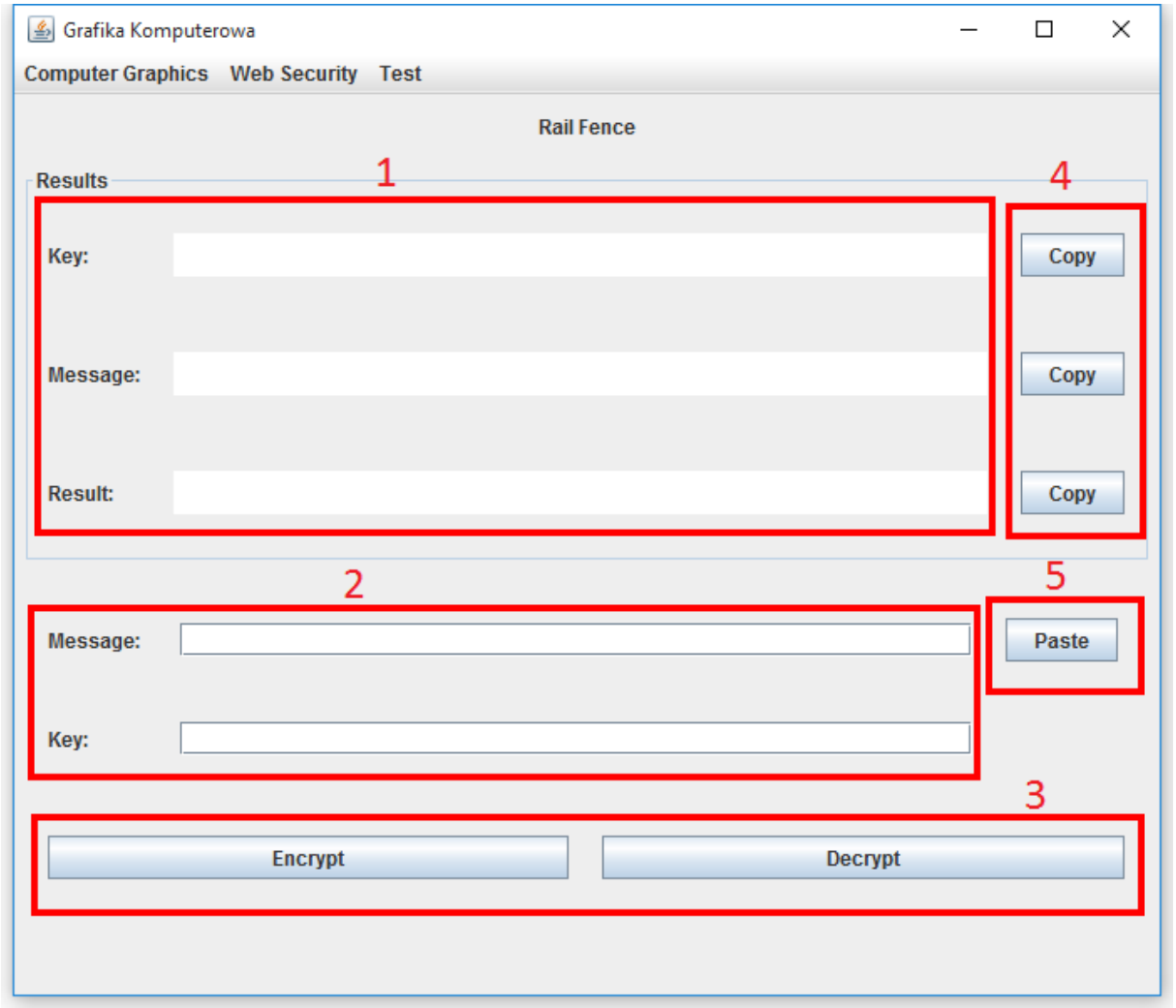
Aby uruchomić program, należy otworzyć plik o nazwie „Grafika Komputerowa.jar” znajdujący się w folderze „bin”.

Wybór algorytmów szyfrujących:

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

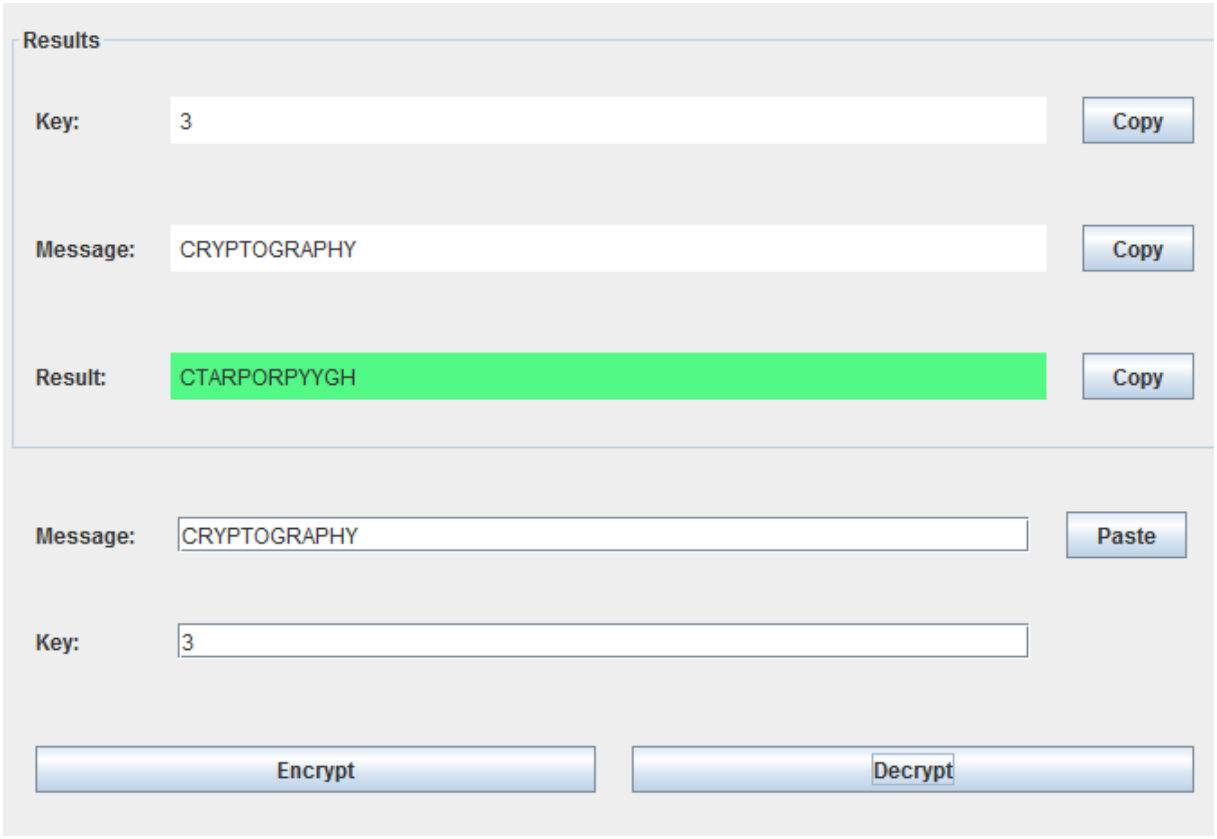


GUI – wyjaśnienie:

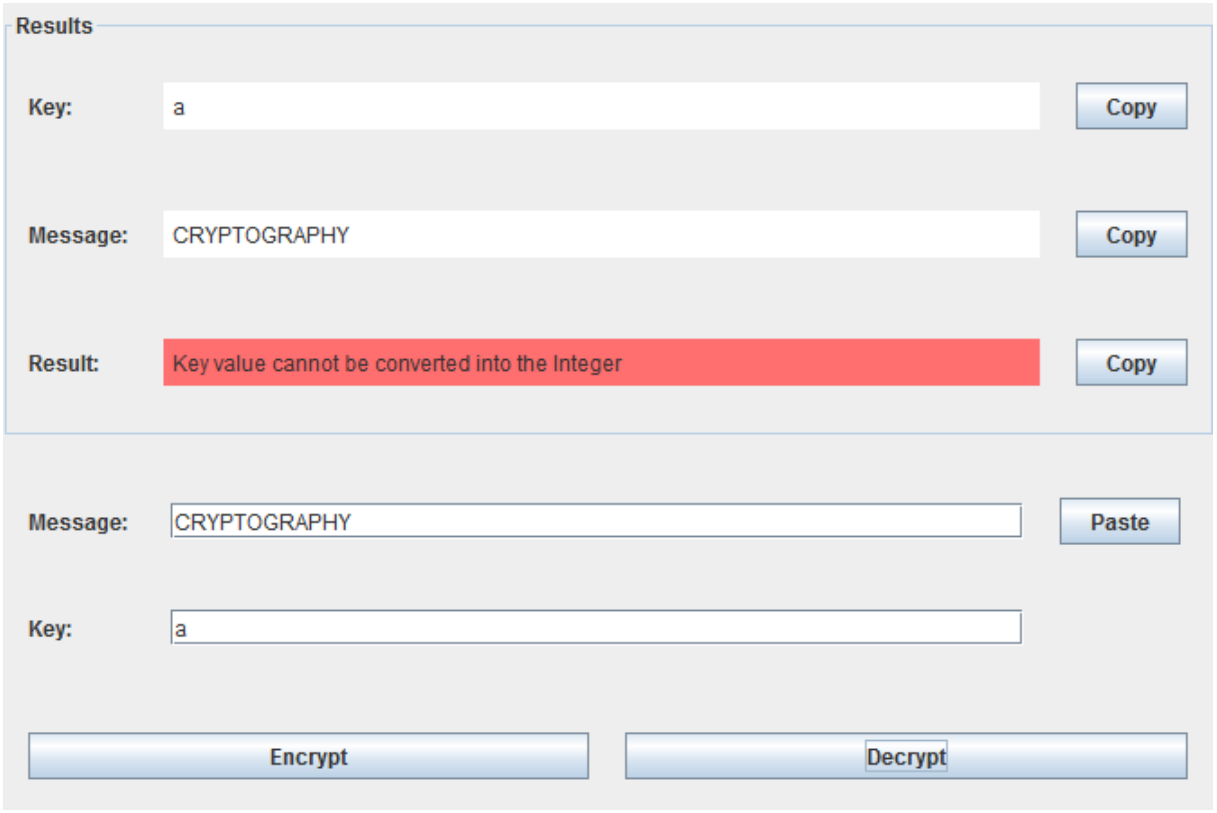


1. Panel, w którym będą wyświetlane wyniki po szyfracji lub deszyfracji.
2. Panel, w którym wpisujemy dane.
3. Panel, w którym wybieramy metodę – szyfrowanie lub deszyfrowanie.
4. Przyciski, które kopiują do schowka systemowego zawartość znajdującą się po ich lewej stronie.
5. Przycisk wklejający zawartość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

M = CRYPTOGRAPHYOSA, key=3-1-4-2

1	2	3	4
C	R	Y	P
T	O	G	R
A	P	H	Y
O	S	A	

C = YCPRGTROHAYPAOS[1]

Zad 3.

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

M=HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION[2]

Key=CONVENIENCE

C	O	N	V	E	N	I	E	N	C	E
1	10	7	11	3	8	6	4	9	2	5
H	E	R	E	I	S	A	S	E	C	R
E	T	M	E	S	S	A	G	E	E	N
C	I	P	H	E	R	E	D	B	Y	T
R	A	N	S	P	O	S	I	T	I	O
N										

C=HECRN CEYI ISEP SGDI RNTO AAES RMPN SSRO EEBT ETIA EEHS[3]

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

C	O	N	V	E	N	I	E	N	C	E
1	10	7	11	3	8	6	4	9	2	5
H										
E	R	E	I	S	A	S	E	C	R	
E	T	M	E	S						
S	A	G	E	E	N	C	I			
P	H	E	R	E	D	B	Y	T	R	A
N	S	P	O	S	I	T				
I	O	N								

C=HEESPNI RR SSEES EIY A SCBT EMGEPN ANDI CT RTAHSO IEERO[4]

Zad 4 (Caesar).

Zaimplementuj szyfr cezara bazujący na podanym przykładzie:

szyfrowanie: $c=(a*k_1+k_0) \bmod n$

deszyfrowanie: $a = [c+(n-k_0)]k_1^{\varphi(n)-1} \bmod n$

dla n=21 $\varphi(n)=12$

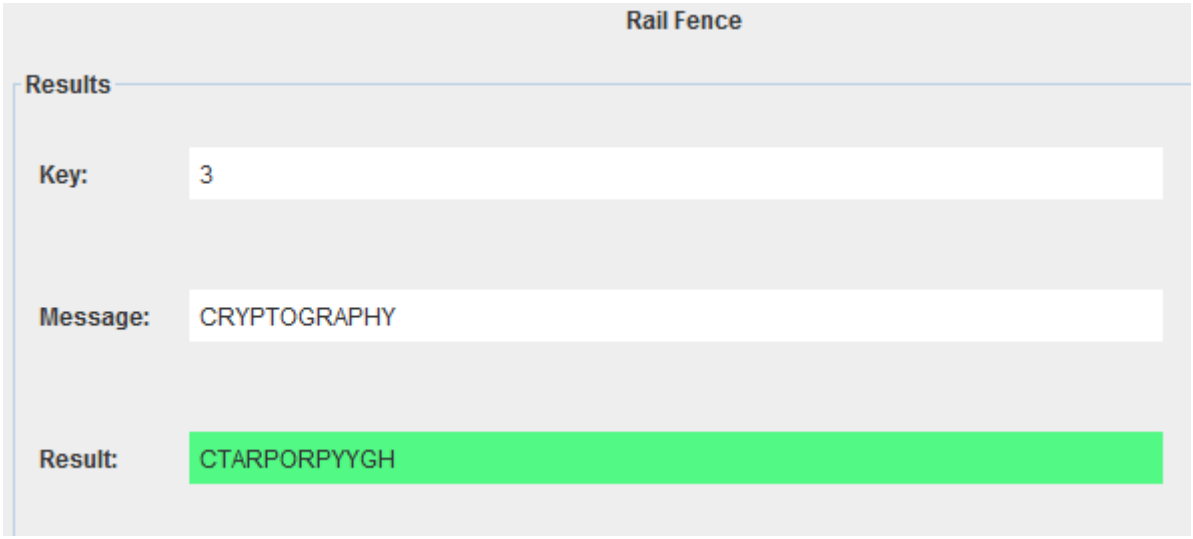
k_1, k_0 muszą być pierwsze względem n.

Zad 5 (Vigenere).

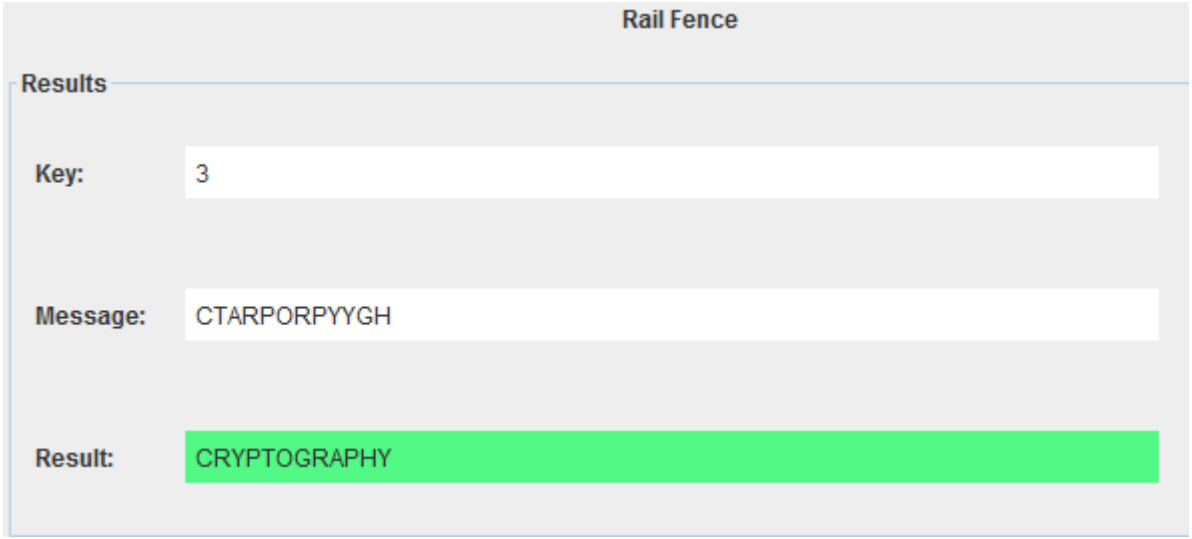
Zaimplementuj kryptosystem bazujący na tablicy Vigenere'a.

Zad 1.

Szyfracja

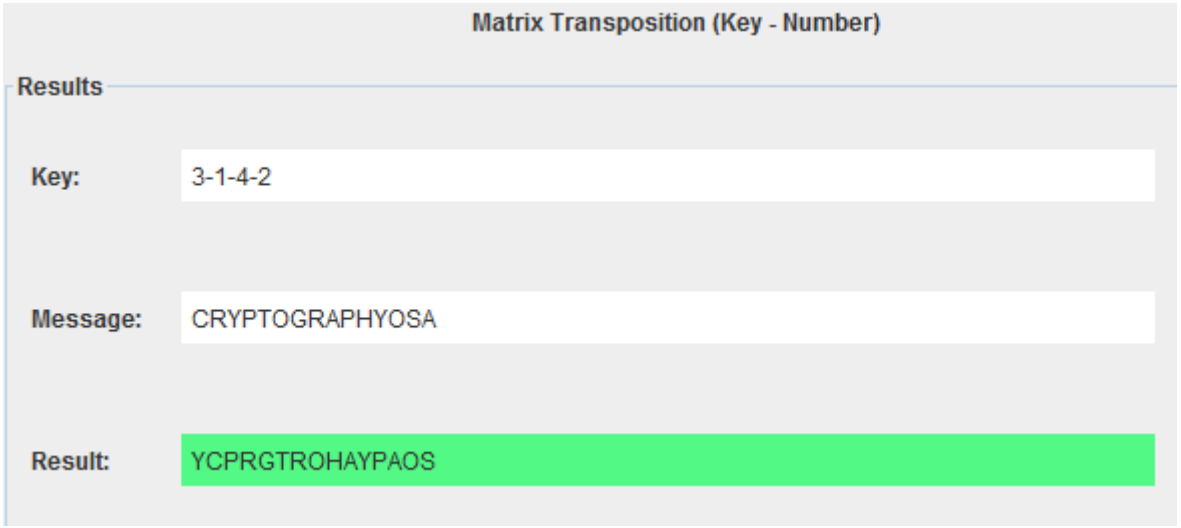


Deszyfracja

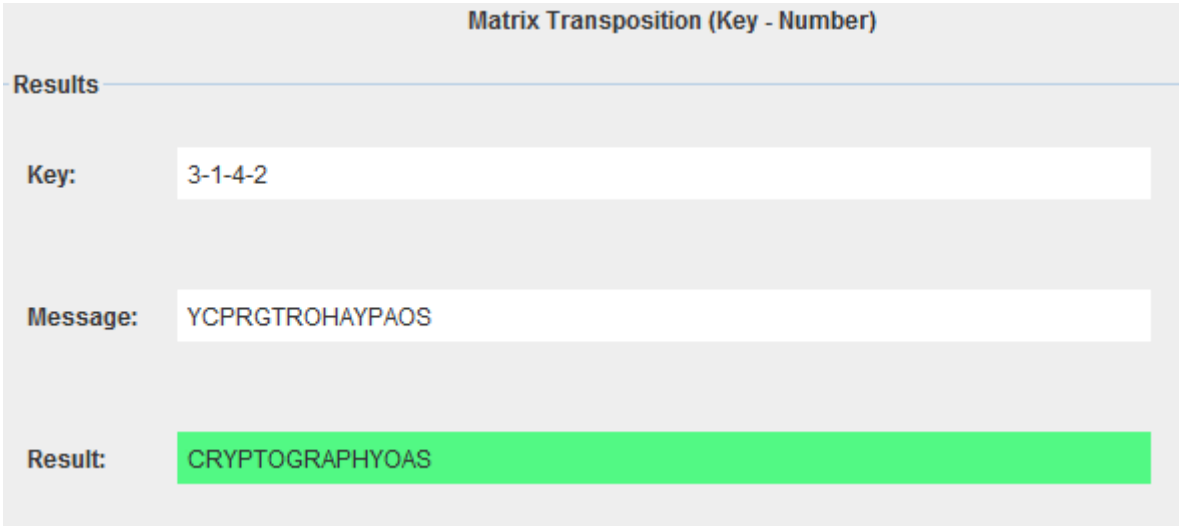


Zad 2

Szyfracja

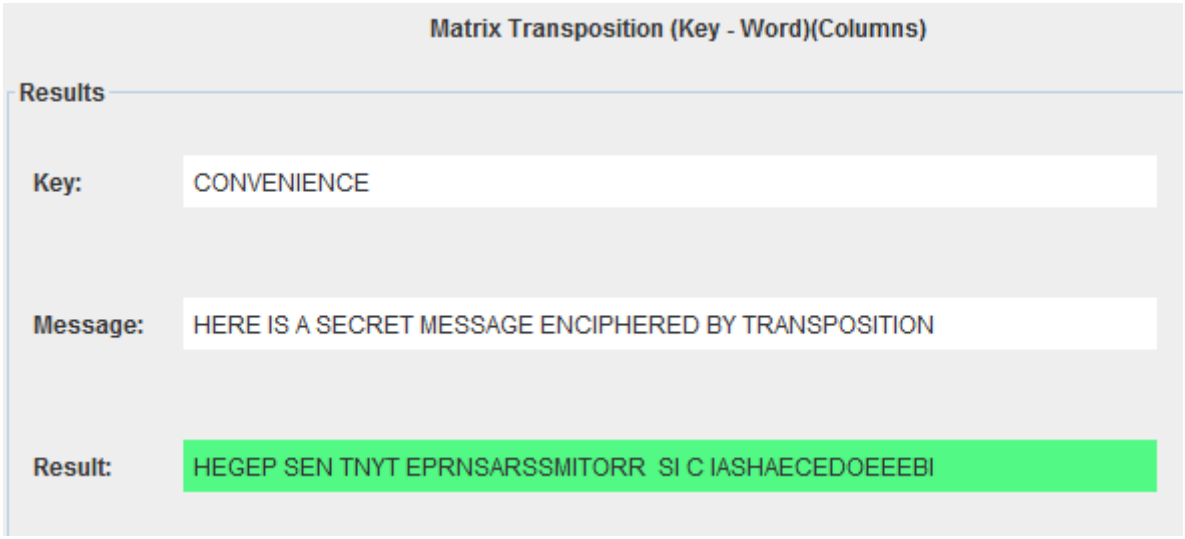


Deszyfracja

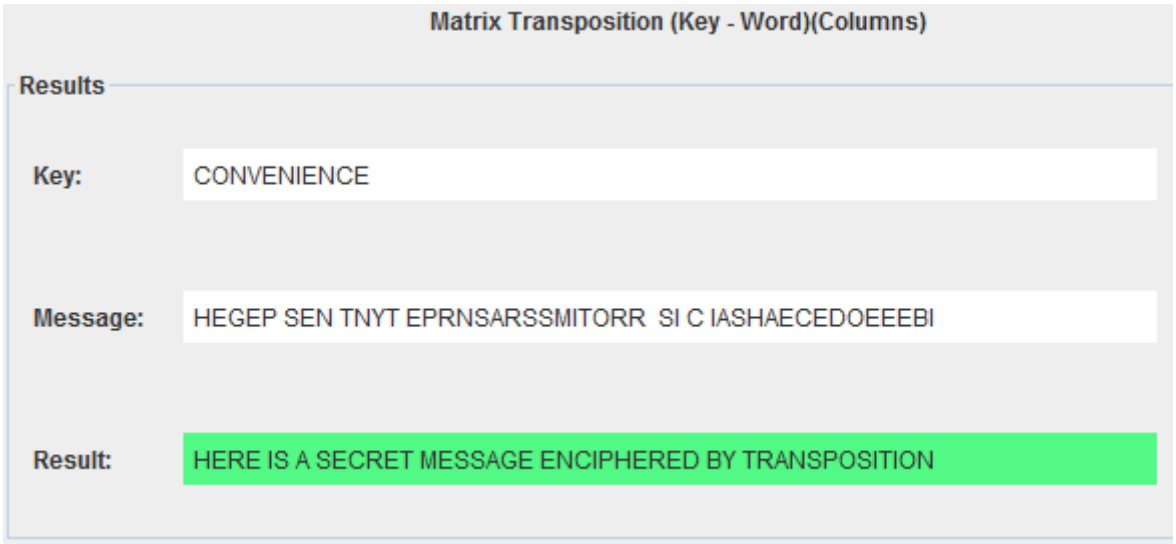


Zad 3 a)

Szyfracja

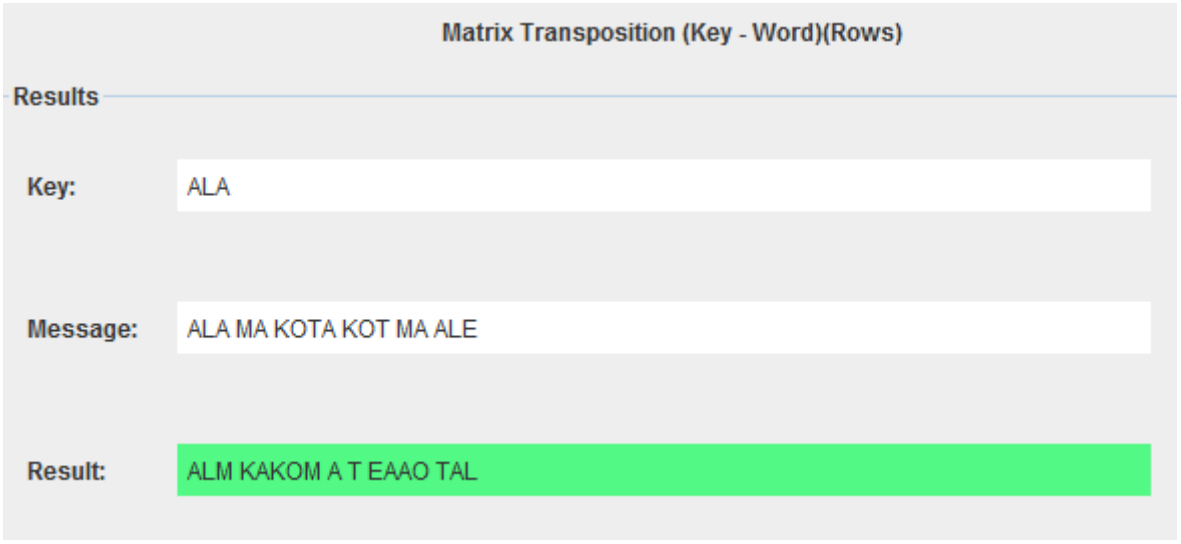


Deszyfracja

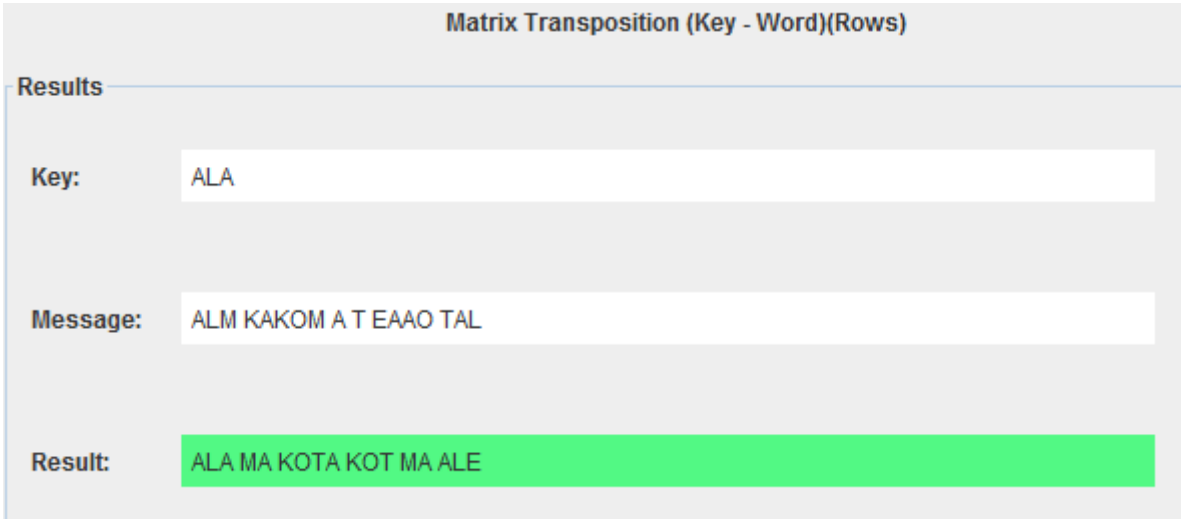


Zad 3 b)

Szyfracja

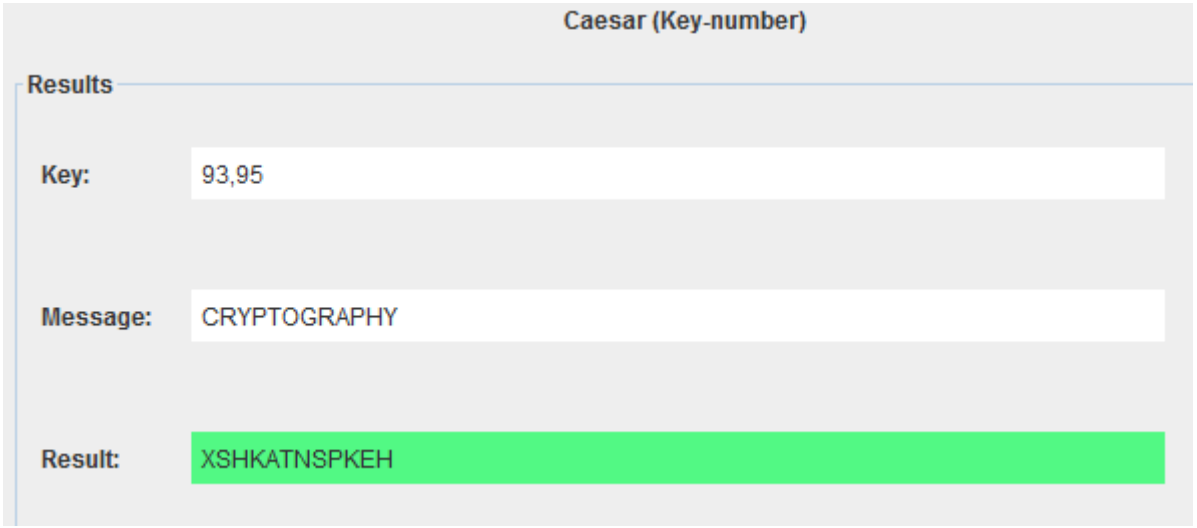


Deszyfracja



Zad 4

Szyfracja



Deszyfracja

Zad 5

Szyfracja

Deszyfracja