

Bezpieczeństwo Sieci Komputerowych	Data: <u>16.03.2016r.</u>
Ćwiczenie nr 1 Autor: <u>Maciej Sawicki</u>	Prowadzący: <u>Dr Inż. Maciej Brzozowski</u>

Środowisko implementacji ćwiczenia:

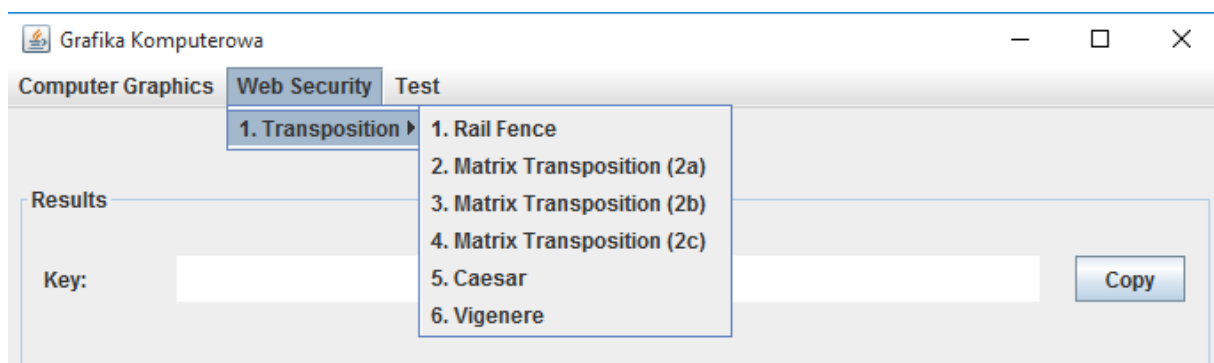
- Java w wersji 1.8.0_51
- NetBeans IDE w wersji 8.1 (Build 201510222201)
- Windows 10 Educational

Uruchomienie:

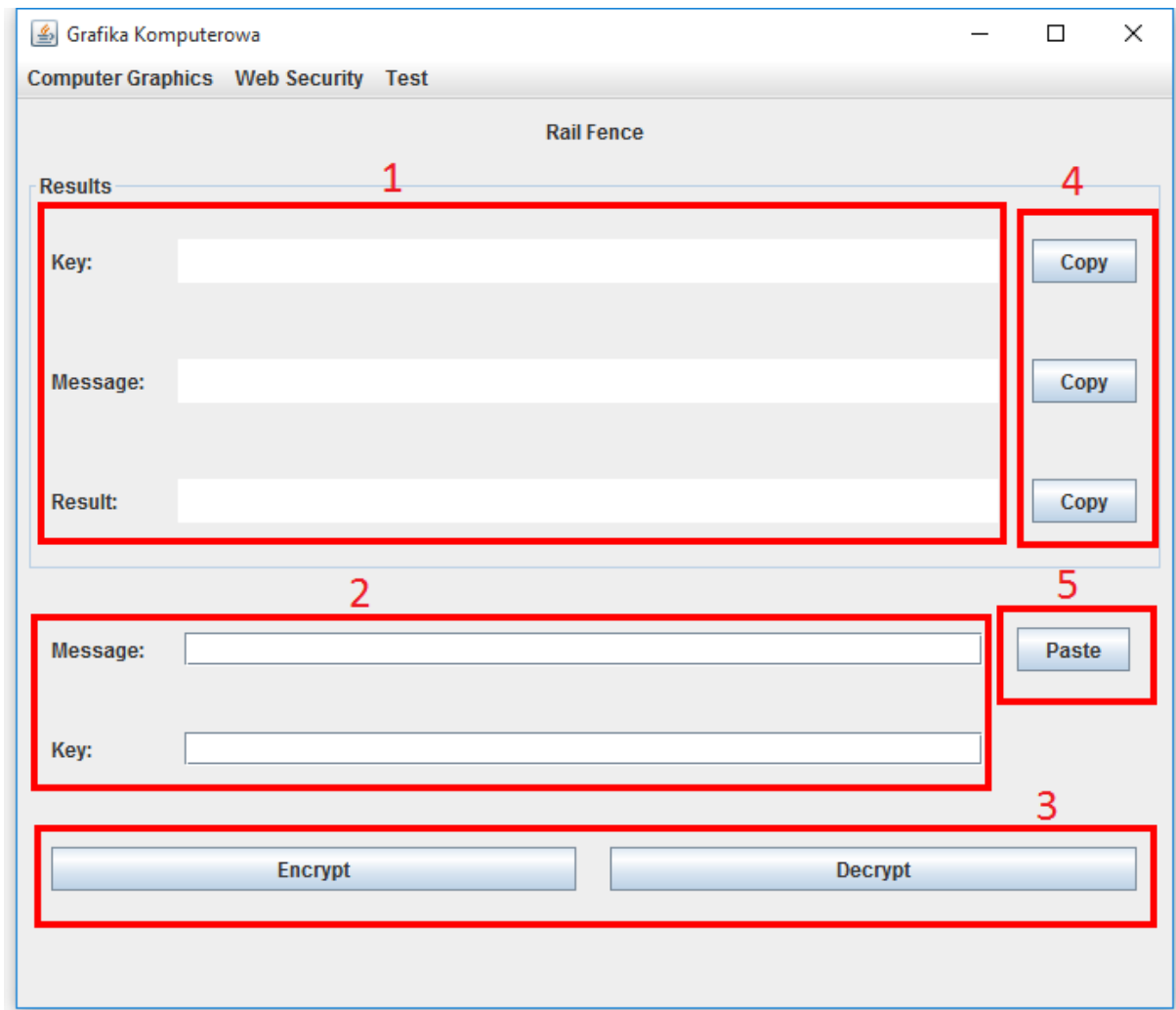
Aby uruchomić program, należy otworzyć plik o nazwie „Grafika Komputerowa.jar” znajdujący się w folderze „bin”.

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:

Results

Key: 3

Copy

Message: CRYPTOGRAPHY

Copy

Result: CTARPORPYYGH

Copy

Message: CRYPTOGRAPHY

Paste

Key: 3

Encrypt

Decrypt

Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:

Results

Key: a

Copy

Message: CRYPTOGRAPHY

Copy

Result: Key value cannot be converted into the Integer

Copy

Message: CRYPTOGRAPHY

Paste

Key: a

Encrypt

Decrypt

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 = YCPRGTROHAYPAOS¹

Zad 3.

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

M=HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION²

Key=CONVENIENCE

[illegible]

C=HECRN CEYI ISEP SGDI RNT0 AAES RMPN SSRO EEBT ETIA EEHS³

- 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 IEERO⁴

Zad 4 (Caesar).

Zaimplementuj szyfr cezara bazujący na podanym przykładzie:

$$\begin{aligned} \text{szyfrowanie: } c &= (a * k_1 + k_0) \bmod n \\ \text{deszyfrowanie: } a &= [c + (n - k_0)] k_1^{\varphi(n)-1} \bmod n \end{aligned}$$

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

Rail Fence	
Results	
Key:	3
Message:	CRYPTOGRAPHY
Result:	CTARPORPYYGH

Deszyfracja

Rail Fence	
Results	
Key:	3
Message:	CTARPORPYYGH
Result:	CRYPTOGRAPHY

Zad 2

Szyfracja

Matrix Transposition (Key - Number)	
Results	
Key:	3-1-4-2
Message:	CRYPTOGRAPHYOSA
Result:	YCPRGTROHAYPAOS

Deszyfracja

Matrix Transposition (Key - Number)	
Results	
Key:	3-1-4-2
Message:	YCPRGTROHAYPAOS
Result:	CRYPTOGRAPHYOAS

Zad 3 a)

Szyfracja

Matrix Transposition (Key - Word)(Columns)	
Results	
Key:	CONVENIENCE
Message:	HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION
Result:	HEGEP SEN TNYT EPRNSARSSMITORR SI C IASHAECEDOEIEBI

Deszyfracja

Matrix Transposition (Key - Word)(Columns)	
Results	
Key:	CONVENIENCE
Message:	HEGEP SEN TNYT EPRNSARSSMITORR SI C IASHAECEDOEIEBI
Result:	HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION

Zad 3 b)

Szyfracja

Matrix Transposition (Key - Word)(Rows)	
Results	
Key:	ALA
Message:	ALA MA KOTA KOT MA ALE
Result:	ALM KAKOM A T EAAO TAL

Deszyfracja

Matrix Transposition (Key - Word)(Rows)	
Results	
Key:	ALA
Message:	ALM KAKOM A T EAAO TAL
Result:	ALA MA KOTA KOT MA ALE

Zad 4

Szyfracja

Caesar (Key-number)	
Results	
Key:	93,95
Message:	CRYPTOGRAPHY
Result:	XSHKATNSPKEH

Deszyfracja

Caesar (Key-number)	
Results	
Key:	93,95
Message:	XSHKATNSPKEH
Result:	CRYPTOGRAPHY

Zad 5

Szyfracja

Vigenere	
Results	
Key:	BREAK
Message:	CRYPTOGRAPHY
Result:	DICPDPXVAZIP

Deszyfracja

Vigenere	
Results	
Key:	BREAK
Message:	DICPDPXVAZIP
Result:	CRYPTOGRAPHY