Bezpieczeństwo Sieci Komputerowych	Data: 15.04.2016r.
Ćwiczenie nr 3 Autor: **Maciej Sawicki**	Prowadzący: Dr Inż. Maciej Brzozowski

Środowisko implementacji ćwiczenia:

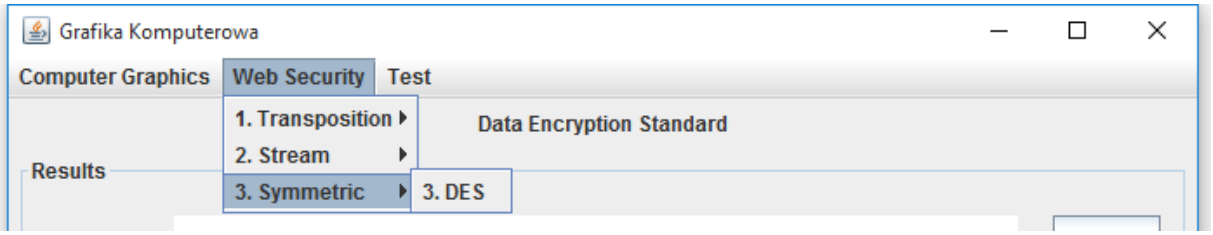
- Java w wersji 1.8.0_51
- NetBeans IDE w wersji 8.1 (Build 201510222201)
- Windows 10 Educational

Uruchomienie:

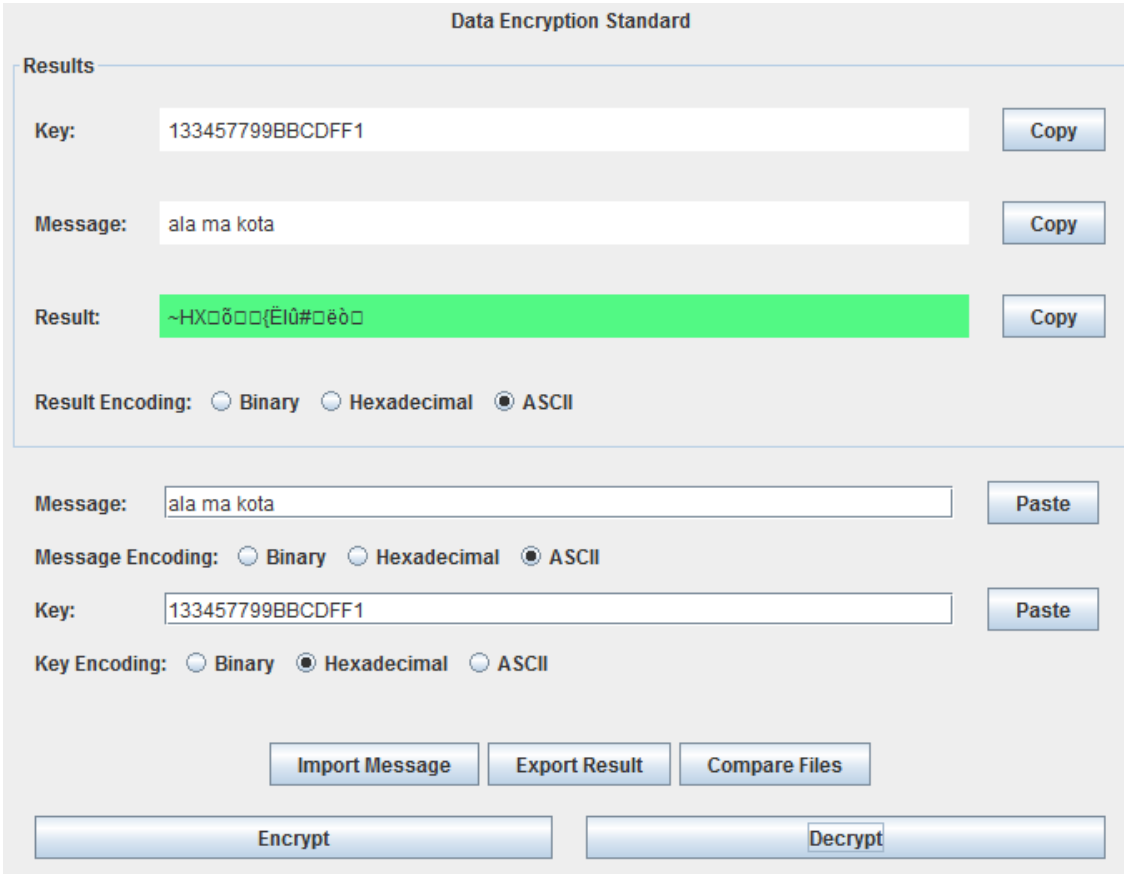
Aby uruchomić program, należy otworzyć plik o nazwie „Grafika Komputerowa.jar” znajdujący się w folderze „bin”.

Wybór algorytmu:

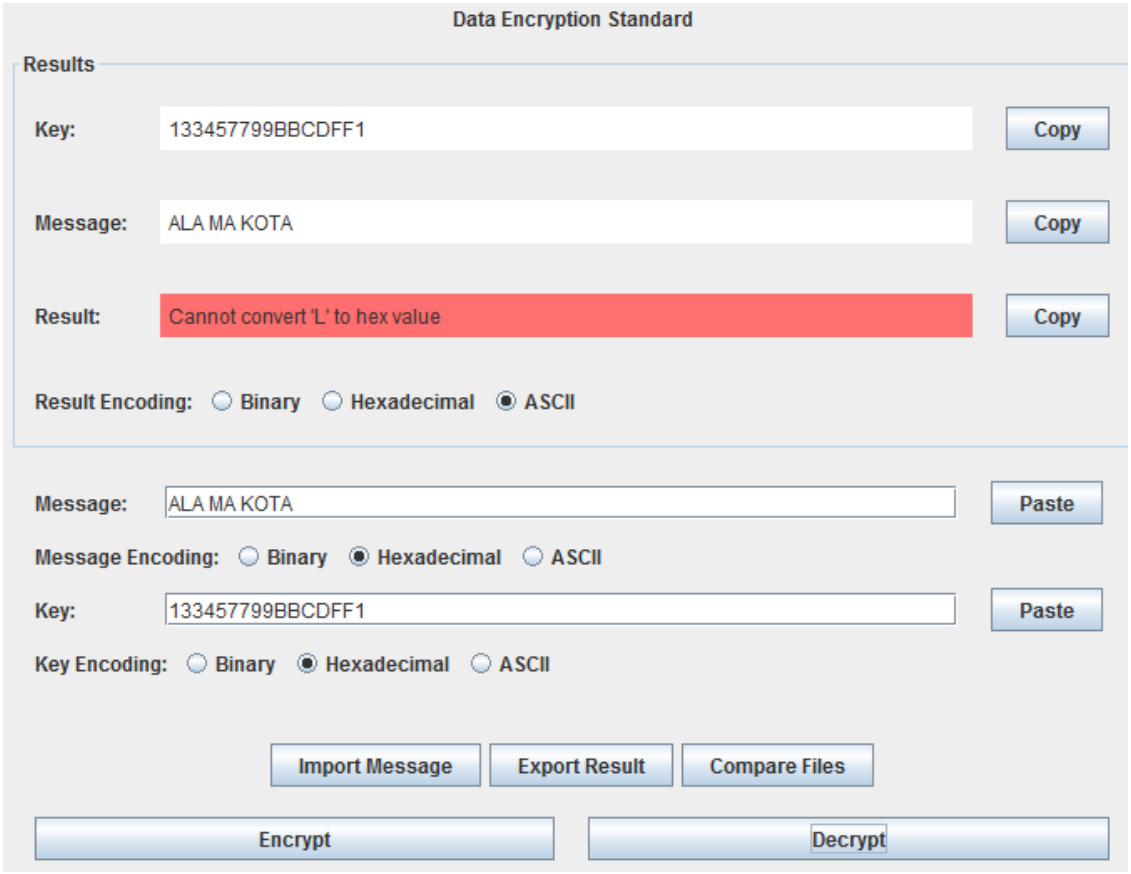
Aby wybrać algorytm DES należy wejść w zakładkę „Web Security”, a następnie w menu „Symmetric” i „DES”.



Przykład POPRAWNIE wykonanego szyfrowania/deszyfrowania:



Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:



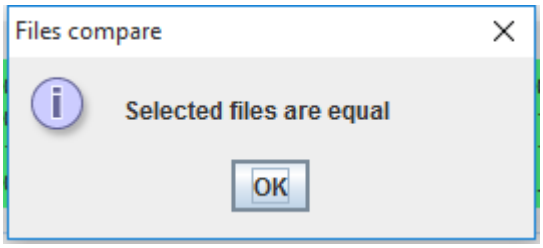
Wczytywanie i zapisywanie i porównywanie plików:

Aby **wczytać** wiadomość do zaszyfrowania w postaci pliku binarnego należy kliknąć przycisk „Import Message”, a następnie wybrać docelowy plik o rozszerzeniu „bin”.

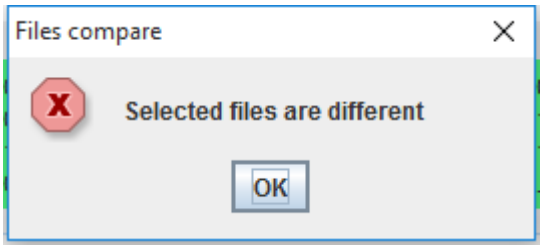
Aby **zapisać** wynik do pliku należy kliknąć przycisk „Export Result”, a następnie wybrać nazwę pliku i kliknąć „Save”.

Aby **porównać** pliki pod względem zawartości należy nacisnąć przycisk „Compare Files”, a następnie zaznaczyć pliki, których zawartość ma zostać porównana.

Jeśli zawartość plików jest taka sama:



Jeśli zawartość plików jest różna:

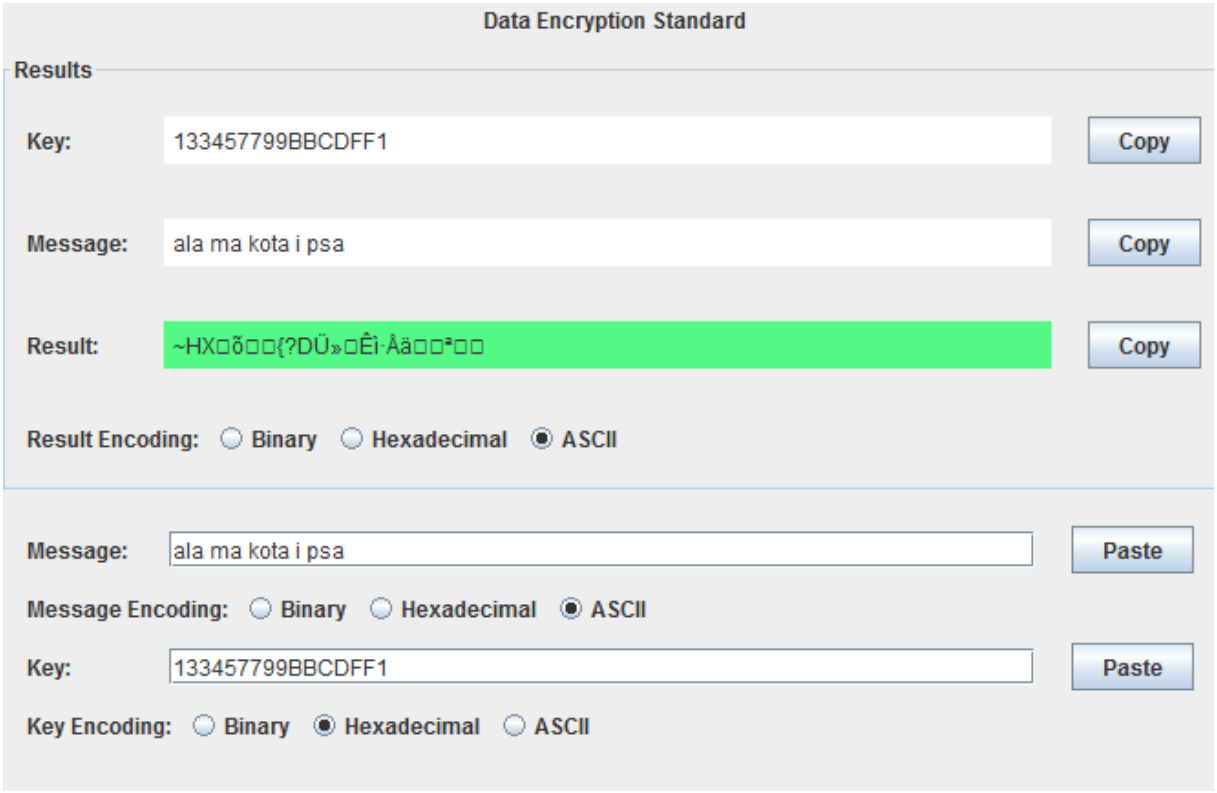


Zadanie:

Wykonaj program realizujący szyfrowanie oraz deszyfrowanie z wykorzystaniem algorytmu DES. Zaimplementuj następujące funkcje:

1. Generowanie kluczy,
2. Funkcja f (R, k),
3. Kolejki,
4. Złączenie w całość komponentów kluczy, funkcji oraz kolejek,
5. Padding informacji przy szyfrowanie i rozszyfrowaniu,
6. Obsługa plików binarnych.

Szyfrowanie wiadomości „ala ma kota i psa”.



Rozszyfrowanie zaszyfrowanej wiadomości.