

Bezpieczeństwo Sieci Komputerowych	Data: <u>15.04.2016r.</u>
Ćwiczenie nr 3 Autor: <u>Maciej Sawicki</u>	Prowadzący: <u>Dr Inż. Maciej Brzozowski</u>

Środowisko implementacji ćwiczenia:

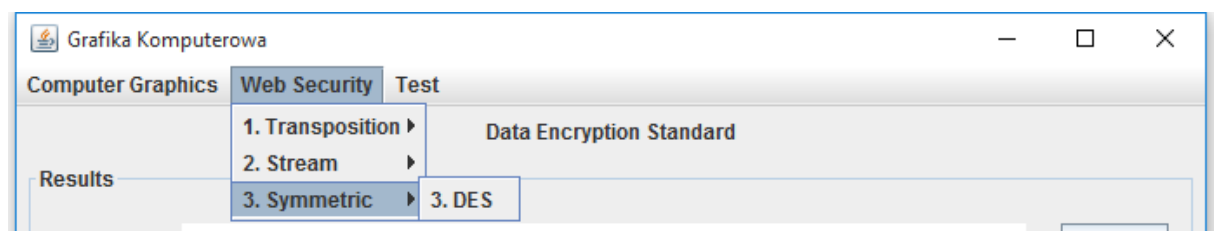
- Java w wersji 1.8.0_51
- NetBeans IDE w wersji 8.1 (Build 201510222201)
- Windows 10 Educational

Uruchomienie:

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

Wybór algorytmu:

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



Przykład POPRAWNIE wykonanego szyfrowania/deszyfrowania:

Data Encryption Standard

Results

Key: 133457799BBCDFF1 Copy

Message: ala ma kota Copy

Result: ~HX□□□□{ÉIû#□ëò□ Copy

Result Encoding: ☐ Binary ☐ Hexadecimal ☒ ASCII

Message: ala ma kota Paste

Message Encoding: ☐ Binary ☐ Hexadecimal ☒ ASCII

Key: 133457799BBCDFF1 Paste

Key Encoding: ☐ Binary ☒ Hexadecimal ☐ ASCII

Import Message Export Result Compare Files

Encrypt Decrypt

Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:

Data Encryption Standard

Results

Key: 133457799BBCDFF1 Copy

Message: ALA MA KOTA Copy

Result: Cannot convert 'L' to hex value Copy

Result Encoding: ☐ Binary ☐ Hexadecimal ☒ ASCII

Message: ALA MA KOTA Paste

Message Encoding: ☐ Binary ☒ Hexadecimal ☐ ASCII

Key: 133457799BBCDFF1 Paste

Key Encoding: ☐ Binary ☒ Hexadecimal ☐ ASCII

Import Message Export Result Compare Files

Encrypt Decrypt

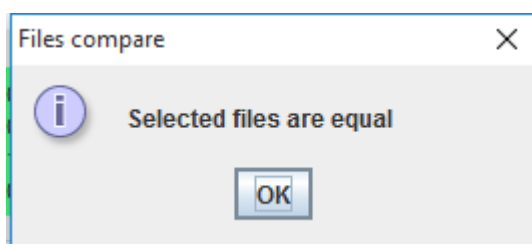
Wczytywanie i zapisywanie i porównywanie plików:

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

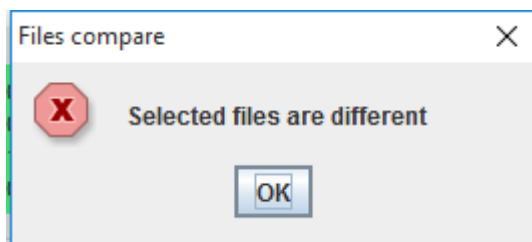
Aby **zapisać** wynik do pliku należy kliknąć przycisk „Export Result”, a następnie wybrać nazwę pliku i kliknąć „Save”.

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 szyfrowaniu i rozszyfrowaniu,
6. Obsługa plików binarnych.

Szyfrowanie wiadomości „ala ma kota i psa”.

Data Encryption Standard

Results

Key:

133457799BBCDFF1

Copy

Message:

ala ma kota i psa

Copy

Result:

~HX    {?DÜ» Êi-Ää  *  

Copy

Result Encoding:

☐ Binary

☐ Hexadecimal

☒ ASCII

Message:

ala ma kota i psa

Paste

Message Encoding:

☐ Binary

☐ Hexadecimal

☒ ASCII

Key:

133457799BBCDFF1

Paste

Key Encoding:

☐ Binary

☒ Hexadecimal

☐ ASCII

Rozszyfrowanie zaszyfrowanej wiadomości.

Data Encryption Standard

Results

Key:133457799BBCDFF1Copy

Message:~HX    {?D              Copy

Result:ala ma kota i psaCopy

Result Encoding: ☐ Binary ☐ Hexadecimal ☒ ASCII

Message:~HX    {?D              Paste

Message Encoding: ☐ Binary ☐ Hexadecimal ☒ ASCII

Key:133457799BBCDFF1Paste

Key Encoding: ☐ Binary ☒ Hexadecimal ☐ ASCII