

| | |
|---|--|
| Bezpieczeństwo Sieci Komputerowych | Data: <u>01.04.2016r.</u> |
| Ćwiczenie nr 2 Autor: <u>Maciej Sawicki</u> | Prowadzący: <u>Dr Inż. Maciej Brzozowski</u> |

Środowisko implementacji ćwiczenia:

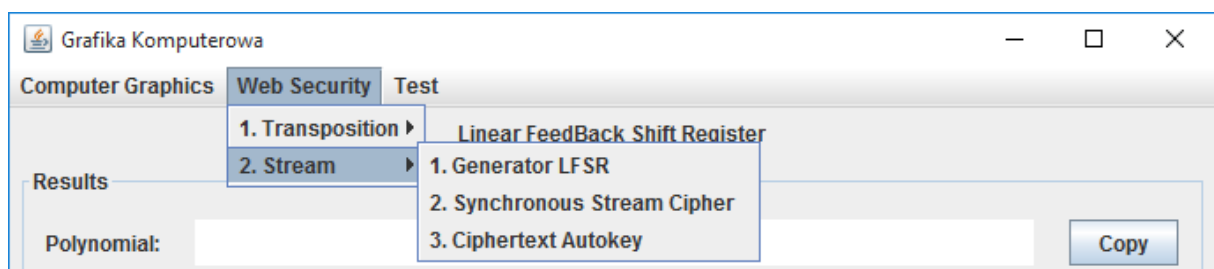
- Java w wersji 1.8.0_51
- NetBeans IDE w wersji 8.1 (Build 201510222201)
- Windows 10 Educational

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 „Stream” i w wybrany algorytm.



Przykład POPRAWNIE wykonanego szyfrowania/deszyfrowania:

| Results | | |
|-------------|-------------------------------------|-------------------------------------|
| Polynomial: | <input type="text" value="1+x+x4"/> | <input type="button" value="Copy"/> |
| Seed: | <input type="text" value="0101"/> | <input type="button" value="Copy"/> |
| Message: | <input type="text" value="1001"/> | <input type="button" value="Copy"/> |
| Length: | <input type="text"/> | <input type="button" value="Copy"/> |
| Result: | <input type="text" value="0101"/> | <input type="button" value="Copy"/> |

| | | |
|-------------|-------------------------------------|--------------------------------------|
| Polynomial: | <input type="text" value="1+x+x4"/> | <input type="button" value="Paste"/> |
| Seed: | <input type="text" value="0101"/> | <input type="button" value="Paste"/> |
| Message: | <input type="text" value="1001"/> | <input type="button" value="Paste"/> |
| Length: | <input type="text"/> | <input type="button" value="Paste"/> |

Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:

| Results | | |
|-------------|--|-------------------------------------|
| Polynomial: | <input type="text" value="1+x+x4"/> | <input type="button" value="Copy"/> |
| Seed: | <input type="text" value="0101"/> | <input type="button" value="Copy"/> |
| Message: | <input type="text" value="10012"/> | <input type="button" value="Copy"/> |
| Length: | <input type="text"/> | <input type="button" value="Copy"/> |
| Result: | <input type="text" value="Parsing Error"/> | <input type="button" value="Copy"/> |

| | | |
|-------------|-------------------------------------|--------------------------------------|
| Polynomial: | <input type="text" value="1+x+x4"/> | <input type="button" value="Paste"/> |
| Seed: | <input type="text" value="0101"/> | <input type="button" value="Paste"/> |
| Message: | <input type="text" value="10012"/> | <input type="button" value="Paste"/> |
| Length: | <input type="text"/> | <input type="button" value="Paste"/> |

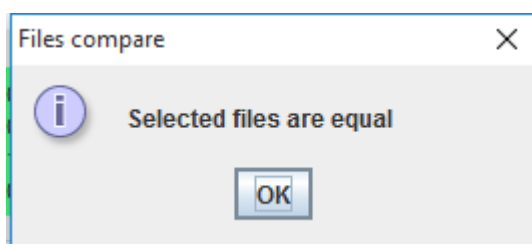
Wczytywanie i zapisywanie i porównywanie plików:

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

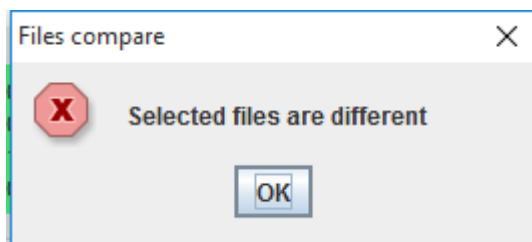
Aby **zapisać** wynik do pliku należy kliknąć przycisk „Export Result”, a następnie wybrać nazwę pliku i kliknąć „Save”.

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:



Zad 1 (Generator LSFR).

Zaimplementuj generator liczb pseudolosowych bazujący na LFSR o zadanym stopniu wielomianu.

Zad 2 (Synchronous Stream Cipher).

Zaimplementuj kryptosystem bazujący na *schemacie Synchronous Stream Cipher* dla podanego wielomianu i ziarna.

Zad 3 (Ciphertext Autokey).

Zaimplementuj kryptosystem bazujący na *schemacie Ciphertext Autokey* dla podanego wielomianu i ziarna.

Zad 1.

Przy generowaniu liczby pseudolosowej jest możliwość ustalenia:

- a) Dowolnej długości liczby, jaka ma zostać wygenerowana („Length”)
- b) Dowolnego wielomianu („Polynomial”)
- c) Dowolnego ziarna („Seed”). Ziarno nie musi mieć długości wielomianu. W razie potrzeby zostanie przycięte, lub wypełnione do wymaganej długości

| Linear FeedBack Shift Register | | |
|--------------------------------|---------------------------|-------|
| Results | | |
| Polynomial: | 1+x+x ⁴ | Copy |
| Seed: | 1001 | Copy |
| Message: | | Copy |
| Length: | 25 | Copy |
| Result: | 0001111010110010001111010 | Copy |
| <hr/> | | |
| Polynomial: | 1+x+x ⁴ | Paste |
| Seed: | 1001 | Paste |
| Message: | | Paste |
| Length: | 25 | Paste |

Rys. Wygenerowana liczba pseudolosowa dla wielomianu: „ $1+x+x^4$ ”, ziarna: „1001”, i wygenerowanej liczby długości „25” bitów.

Zad 2.

Szyfracja dla wielomianu: „ $1+x+x^4$ ”, ziarna: „0101”, oraz wiadomości: „**10011100**”.

| Synchronous Stream Cipher | | |
|---------------------------|----------|-------|
| Results | | |
| Polynomial: | 1+x+x4 | Copy |
| Seed: | 0101 | Copy |
| Message: | 10011100 | Copy |
| Length: | | Copy |
| Result: | 01010100 | Copy |
| Polynomial: | 1+x+x4 | Paste |
| Seed: | 0101 | Paste |
| Message: | 10011100 | Paste |
| Length: | | Paste |

Deszyfracja dla wielomianu: „ $1+x+x^4$ ”, ziarna: „0101”, oraz wiadomości: „**01010100**”.

| Synchronous Stream Cipher | | |
|---------------------------|----------|-------|
| Results | | |
| Polynomial: | 1+x+x4 | Copy |
| Seed: | 0101 | Copy |
| Message: | 01010100 | Copy |
| Length: | | Copy |
| Result: | 10011100 | Copy |
| Polynomial: | 1+x+x4 | Paste |
| Seed: | 0101 | Paste |
| Message: | 01010100 | Paste |
| Length: | | Paste |

Zad 3.

Szyfracja dla wielomianu: „ $1+x+x^4$ ”, ziarna: „1100”, oraz wiadomości: „11010100”.

| Ciphertext Autokey | | |
|--------------------|----------|------|
| Results | | |
| Polynomial: | 1+x+x4 | Copy |
| Seed: | 1100 | Copy |
| Message: | 11010100 | Copy |
| Length: | | Copy |
| Result: | 01000000 | Copy |

| | | |
|-------------|----------|-------|
| Polynomial: | 1+x+x4 | Paste |
| Seed: | 1100 | Paste |
| Message: | 11010100 | Paste |
| Length: | | Paste |

Deszyfracja dla wielomianu: „ $1+x+x^4$ ”, ziarna: „1100”, oraz wiadomości: „01000000”.

| Ciphertext Autokey | | |
|--------------------|----------|------|
| Results | | |
| Polynomial: | 1+x+x4 | Copy |
| Seed: | 1100 | Copy |
| Message: | 01000000 | Copy |
| Length: | | Copy |
| Result: | 11010100 | Copy |

| | | |
|-------------|----------|-------|
| Polynomial: | 1+x+x4 | Paste |
| Seed: | 1100 | Paste |
| Message: | 01000000 | Paste |
| Length: | | Paste |