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

Środowisko implementacji ćwiczenia:

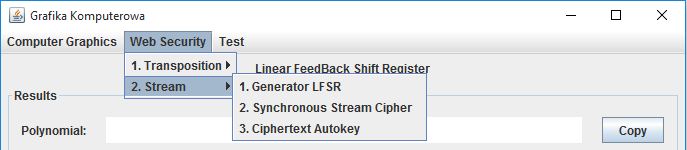
* Java w wersji 1.8.0\_51
* NetBeans IDE w wersji 8.1 (Build 201510222201)
* Windows 10 Educational

Uruchomienie:

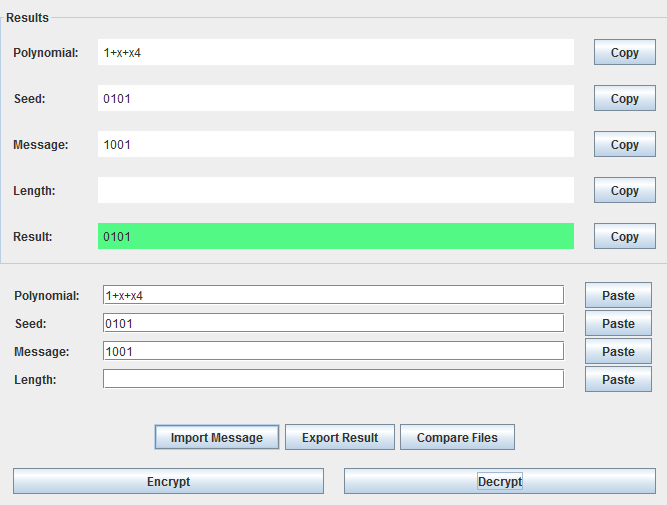
Aby uruchomić program, należy otworzyć plik o nazwie „Grafika Komputerowa.jar” znajdujący się w folderze „bin”.

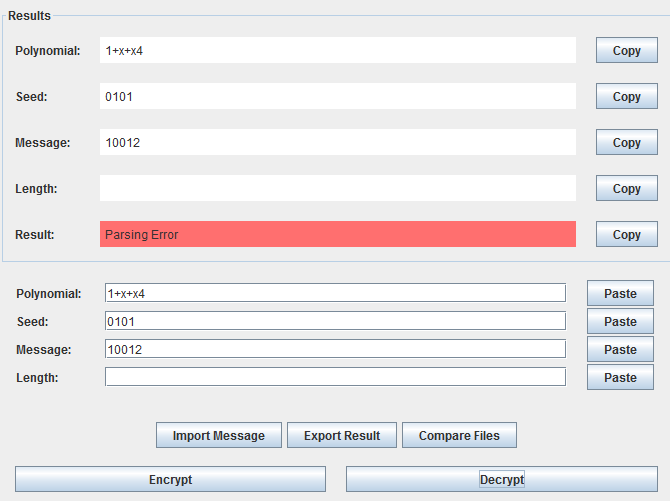
Wybór algorytmów szyfrujących:

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



Przykład POPRAWNIE wykonanego szyfrowania/deszyfrowania:



Przykład NIEPOPRAWNIE wykonanego szyfrowania/deszyfrowania:

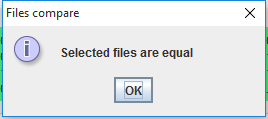
Wczytywanie i zapisywanie i porównywanie plików:

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

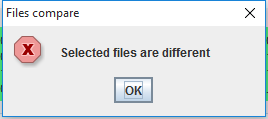
Aby **zapisać** wynik do pliku należy kliknąć przycisk „Export Result”, a następnie wybrać nazwę pliku i kliknąć „Save”.

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:



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 Ciper* dla podanego wielomianu i ziarna.

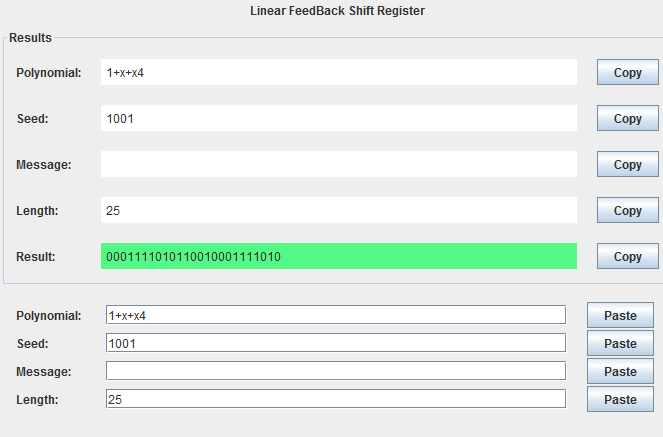
Zad 3 (Ciphertext Autokey).

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

Zad 1.

Przy generowaniu liczby pseudolosowej jest możliwość ustalenia:

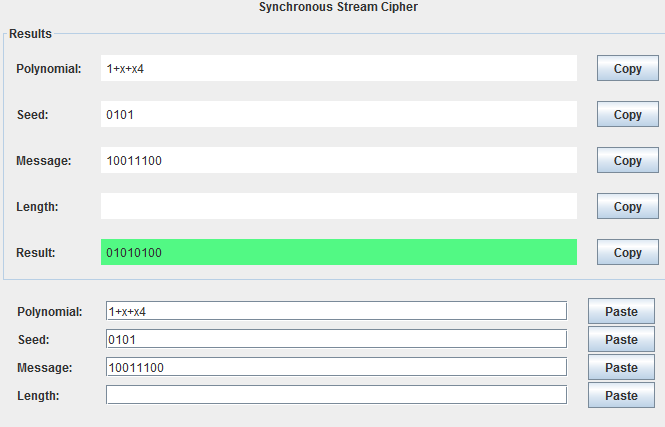
1. Dowolnej długości liczby, jaka ma zostać wygenerowana („Length”)
2. Dowolnego wielomianu („Polynomial”)
3. Dowolnego ziarna („Seed”). Ziarno nie musi mieć długości wielomianu. W razie potrzeby zostanie przycięte, lub wypełnione do wymaganej długości



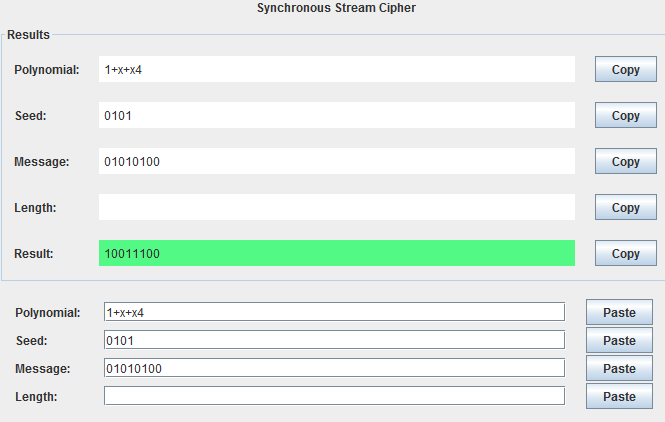
*Rys. Wygenerowana liczba pseudolosowa dla wielomianu: „1+x+x^4”, ziarna: „1001”, i wygenerowanej liczby długości „25” bitów.*

Zad 2.

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

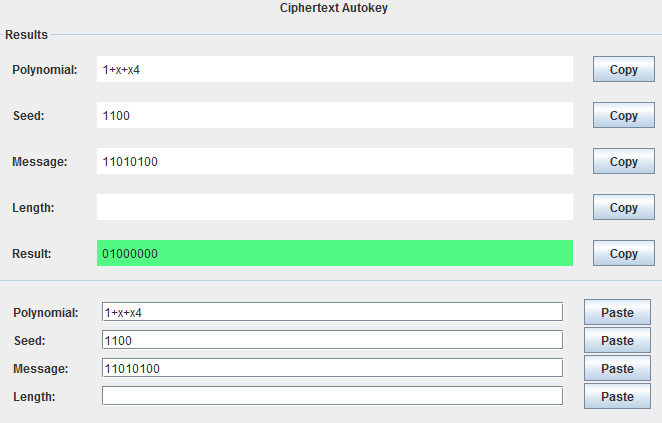


Deszyfracja dla wielomianu: „1+x+x^4”, ziarna: „0101”, oraz wiadomości: „**01010100**”.



Zad 3.

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



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

