Sprawozdanie nr 2

z przedmiotu Wybrane Elementy Kryptologii

- **Zadania do realizacji w sprawozdaniu**

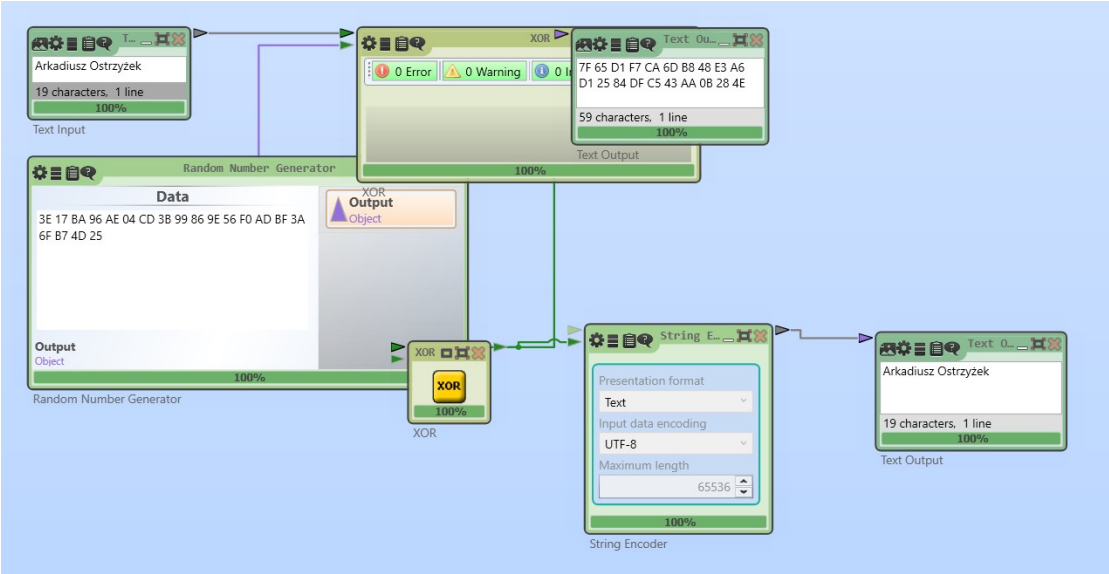
1. Szyfr z kluczem jednokrotnym – OTP (*One Time Pad*)

a)

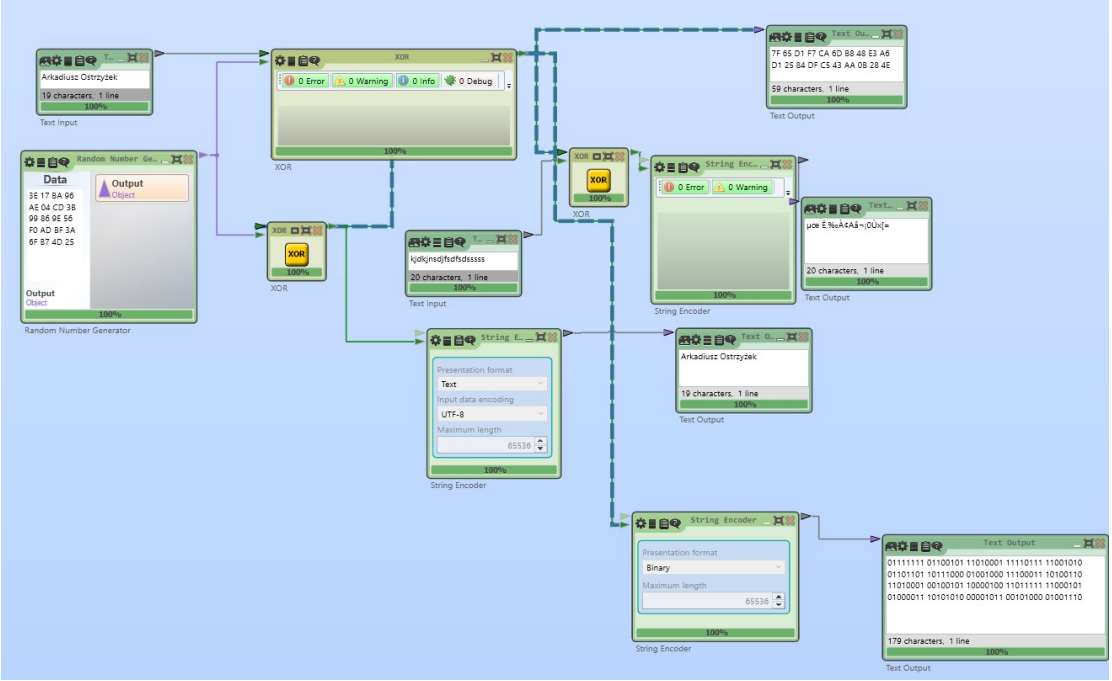
Tekst jawny: Arkadiusz Ostrzyżek

Wygenerowany klucz: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25

Zaszyfrowana wiadomość: 7F 65 D1 F7 CA 6D B8 48 E3 A6 D1 25 84 DF C5 43 AA 0B 28 4E

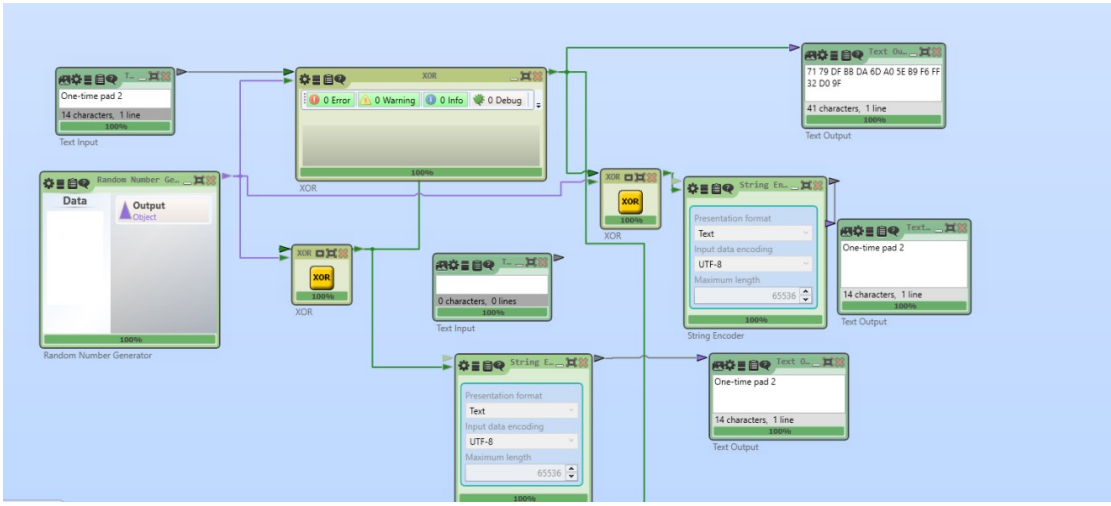


b)



Wartość klucza: kjdkjnsdjfsdfsdssssss
Szyfrogram: µœ Ë,‰ÀAâ¬¡0Ùx[=

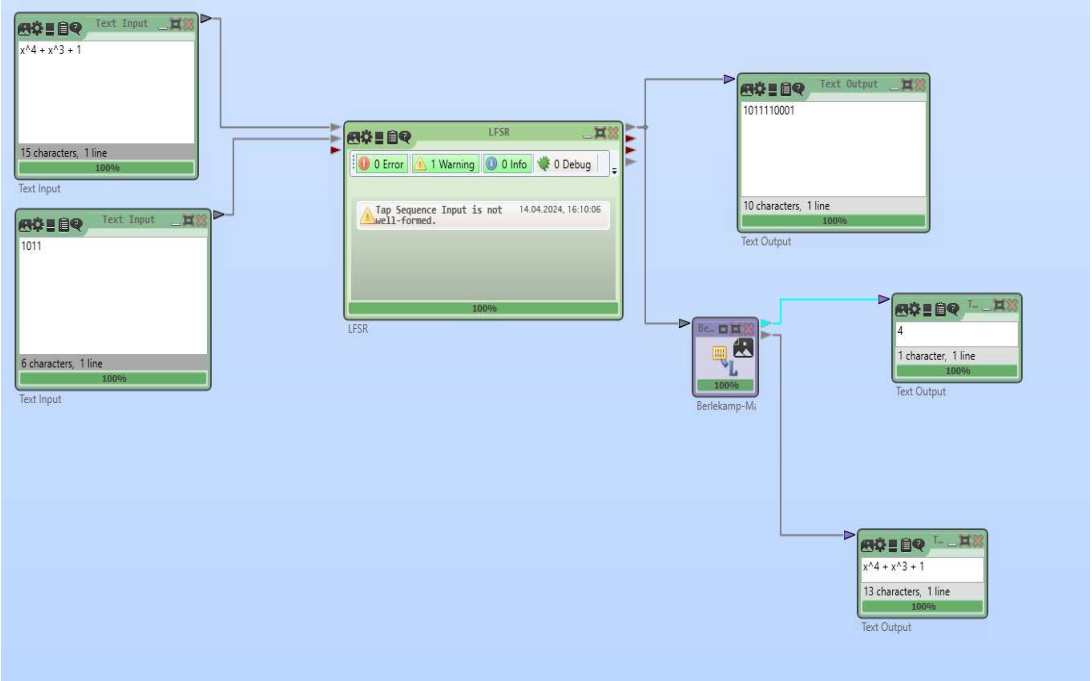
Ewentualnie:



Można odszyfrować, aby uzyskać sensowny tekst jawny.

2. Rejestr LFSR i atak na niego

a)



b) Berkerley-Massey znalazł stopień i wielomian oznaczajacy najmniejszy mozliwy LSFR, który osiądnie na uzyskanie tego wyniku.

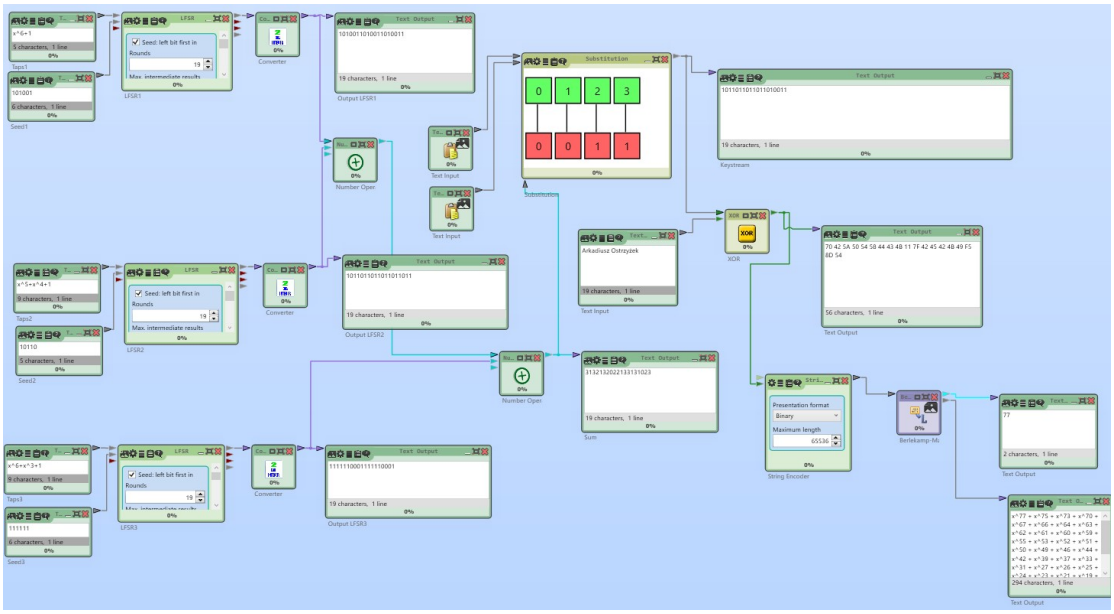
3. Pzykład generatora zbudowanego na bazie rejestru LFSR

a)

Tekst jawny: Arkadiusz Ostrzyżek

Klucz: 1010011010011010011

Szyfrogram: 70 42 5A 50 54 58 44 43 4B 11 7F 42 45 42 4B 49 F5 8D 54



b)

Wielomian będzie dłuższy od pojedynczego wyniku LFSR

4. Szyfr strumieniowy Trivium

a)

Tekst jawny: Arkadiusz Ostrzyżek

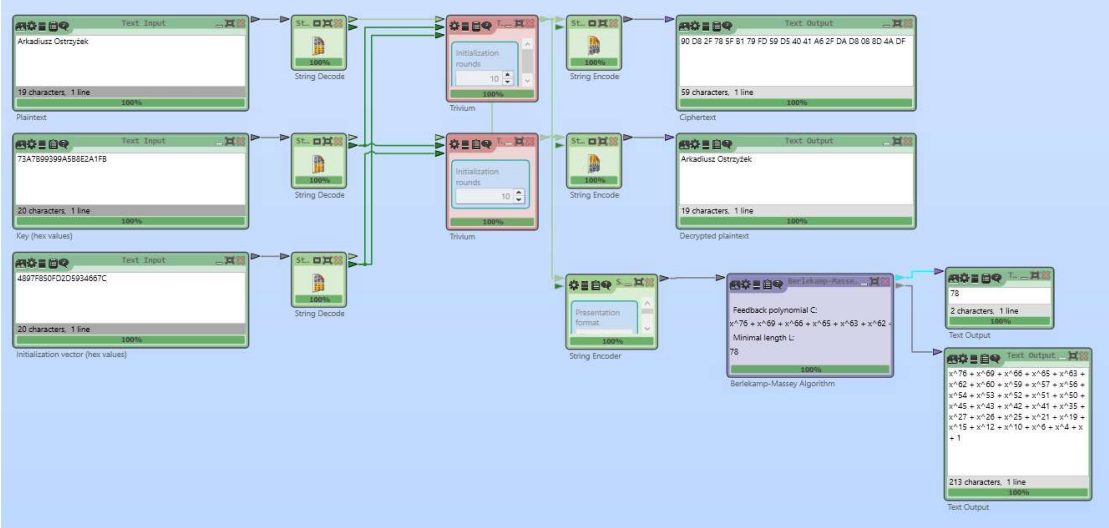
Klucz: 73A7B99399A5B8E2A1FB

Szyfrogram: 90 D8 2F 78 5F B1 79 FD 59 D5 40 41 A6 2F DA D8 08 8D 4A DF

Odzyskany tekst jawny: Arkadiusz Ostrzyżek

b)

LFSR jest linearny, Trivium jest nielinearny. Im dłuższy klucz, tym dłuższy wielomian.



c) Wypisz nazwy innych szyfrów strumieniowych, które są dostępne w programie CrypTool.

1. RC4

2. Trivium

3. Grain-128

4. HC-128

5 Salsa20

6 Rabbit