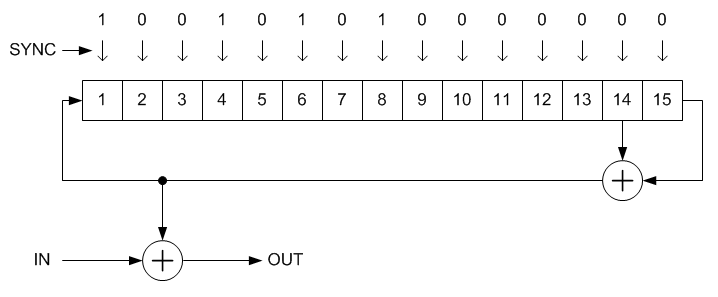
|  |  |  |  |
| --- | --- | --- | --- |
| Niezawodność i diagnostyka układów cyfrowych 2 | | | |
| **Scrambling** | | | |
| Termin zajęć | Poniedziałek TP,  9:15 – 11:00 | Wersja | 1 |
| Skład grupy | | Prowadzący | |
| Grzegorz Cyganiuk, 234928 Michał Madarasz, 238903  Mateusz Stafiniak, 234937 | | mgr inż. Piotr Semberecki | |

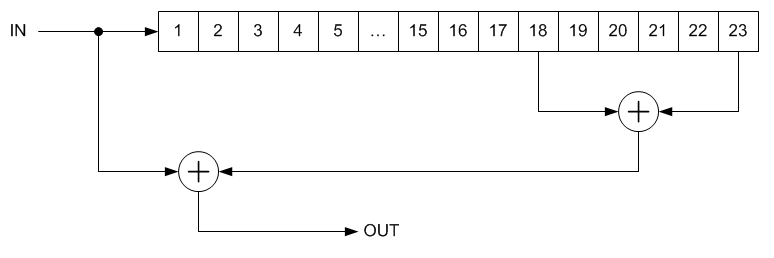
# Scrambler

Scrambler jest to urządzenie, które za zadanie ma randomizację sekwencji bitowych, aby wyrównać średnią ilość zer i jedynek oraz w jak najmniejszym stopniu doprowadzać do sytuacji takiej, że tworzą się długie ciągi zer lub jedynek. Takie zjawisko doprowadziłoby do desynchronizacji urządzeń. Wyróżniamy dwa typy scramblera: addytywny oraz multiplikatywny. Pierwszy z nich opisany, jako scrambler synchroniczny wykorzystuje tzw. rejestr przesuwny ze sprzężeniem zwrotnym (LFSR). Aby ten konkretny rodzaj scramblera nie tracił synchronizacji, stosuje się, co jakiś czas kolejne punkty synchronizujące gdzie występuje tzw. SYNC-WORD, czyli stały punkt synchronizacji.

Poniżej znajduje się obrazek addytywnego scramblera o wielomianie   
1 + x-14 + x-15, wykorzystanego w DVB.

Drugi rodzaj scramblera (multiplikatywny) to scrambler samo-synchronizujący. W przeciwieństwie do scramblera addytywnego, ten rodzaj nie posiada ramki synchronizującej, wspomnianego wcześniej SYNC-WORD.

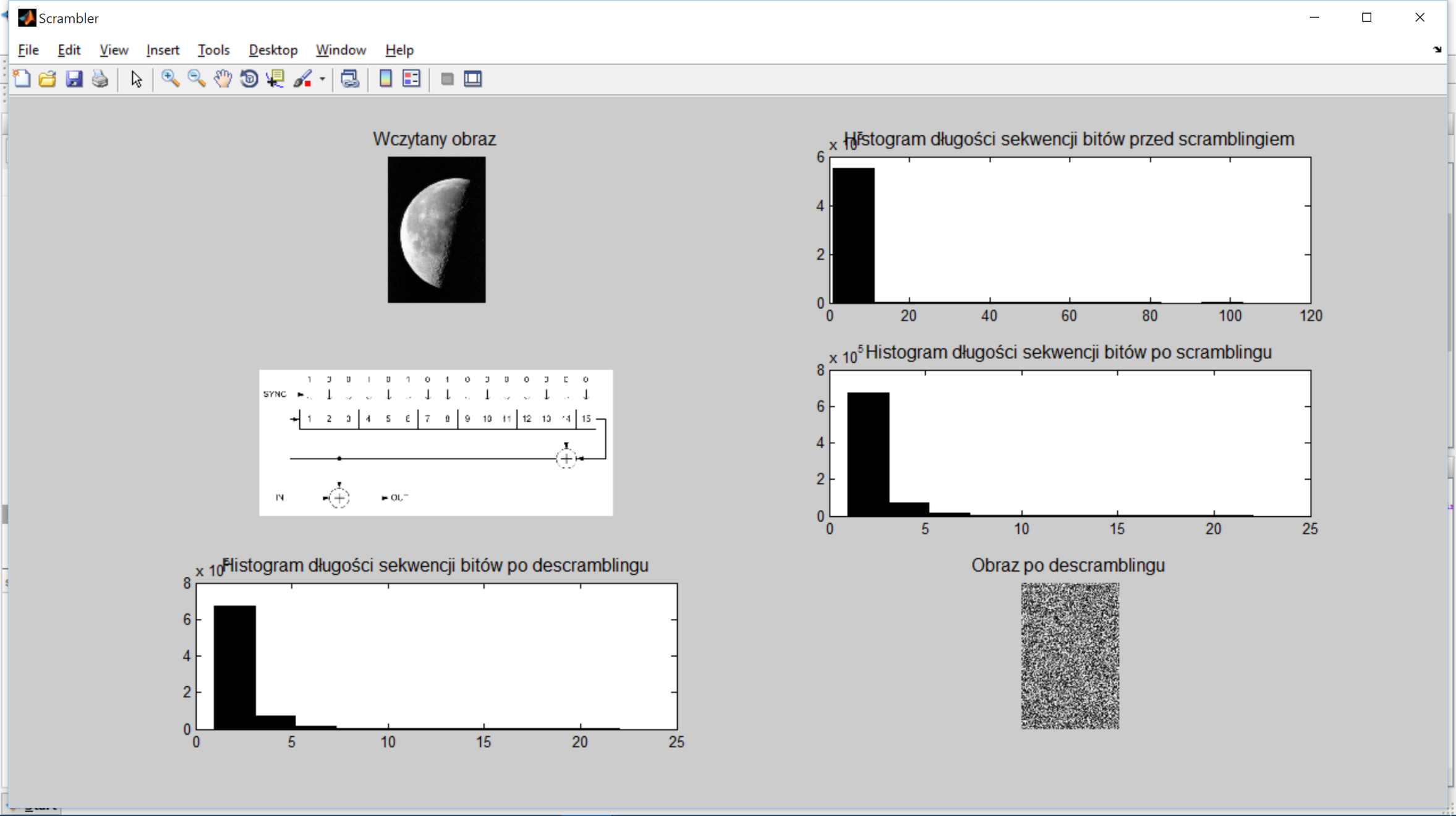
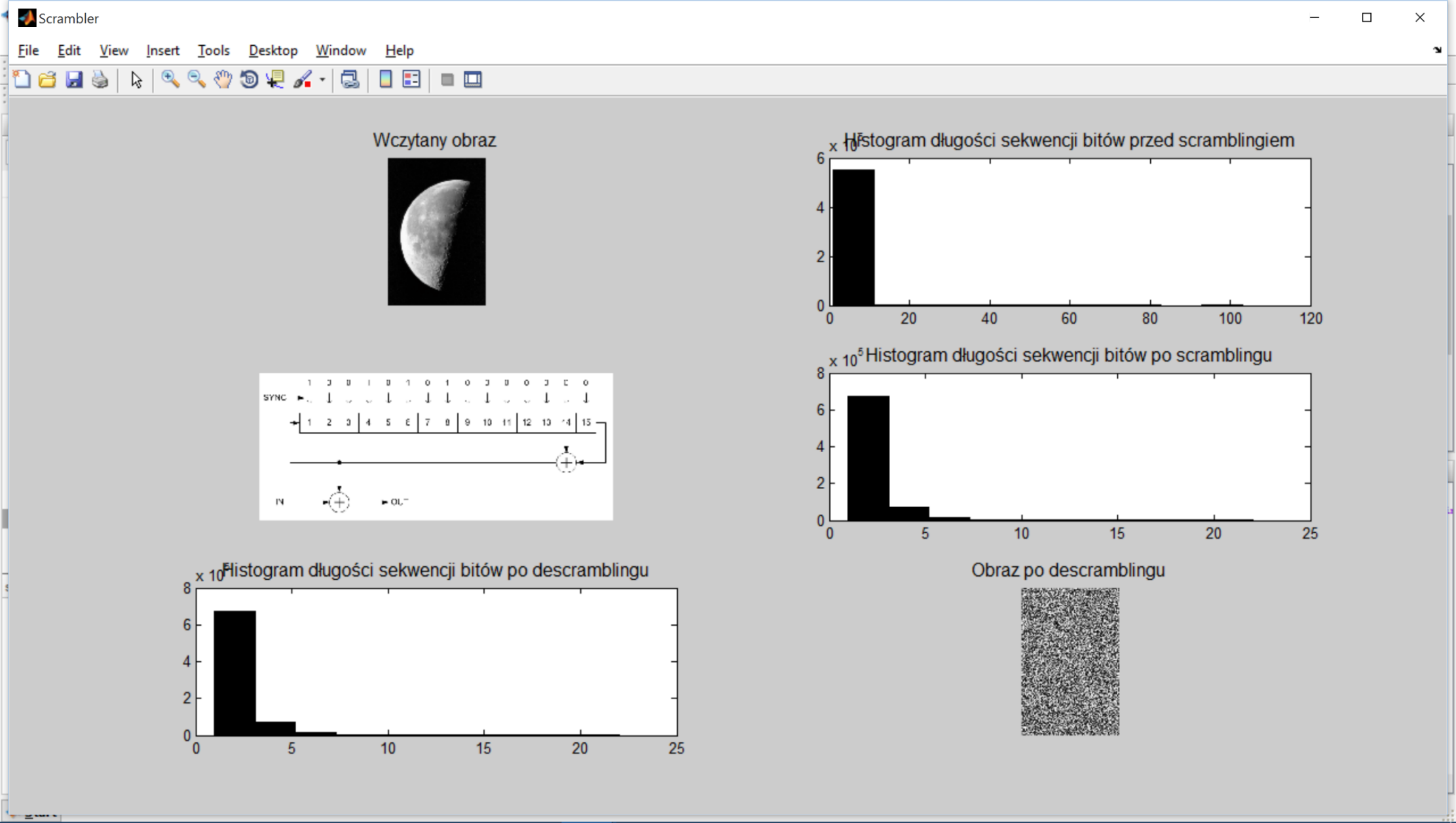
Poniżej został przedstawiony obrazek scramblera multiplikatywnego   
o wielomianie 1 + x-18 + x-23.



# Zastosowanie scrablera

Scrambler szybko znalazł zastosowanie nie tylko w eliminacji niechcianych, długich ciągów bitów, ale także jest używany w szyfrowaniu np. w telewizji prepaid view, czy w telewizji cyfrowej. Jednym z algorytmów szyfrujących jest CSA (Common Scrambling Algorithm), służący do szyfrowania przekazu telewizji cyfrowej DVB. Bez takiego algorytmu każdy użytkownik mógłby odbierać sygnał telewizyjny płatnej telewizji i za niego nie płacić, dzięki temu algorytmowi nie jest to możliwe.

# Descrambler

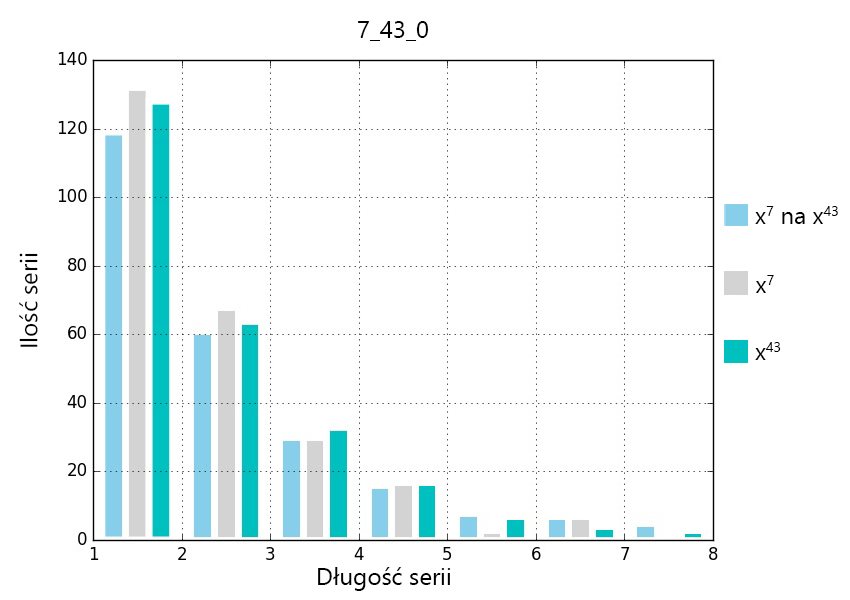
Descrambler jest urządzeniem odwrotnym do scramblera. Posiada ten sam klucz i odkodowuje sygnały bitowe do naszego urządzenia końcowego. Poniżej przedstawiony został obrazek, kiedy scrambler ma całkiem inny wielomian niż descrambler, sytuacja taka może się zdarzyć, gdy ktoś próbuje nielegalnie oglądać kodowane sygnały i sprawdza wszystkie możliwości klucza descramblera.

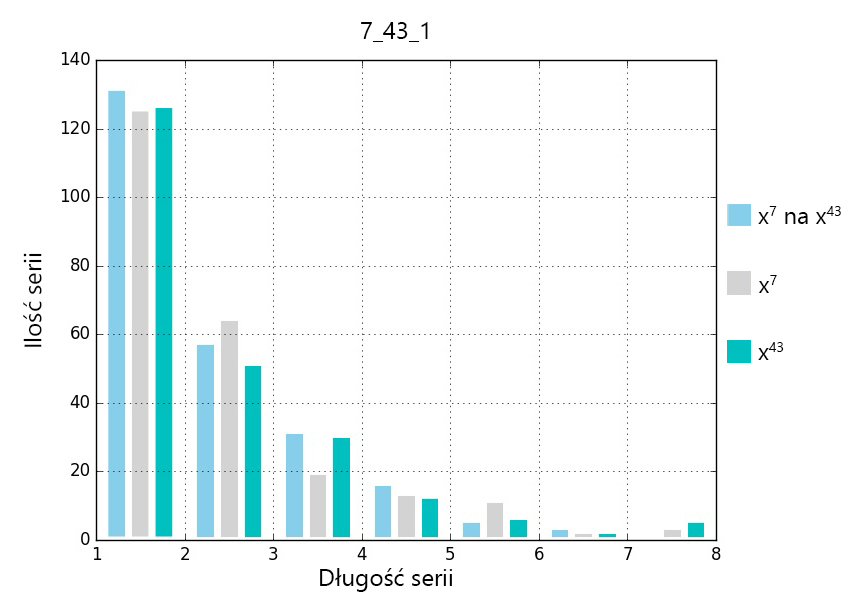
# Wady scramblerów

- oba typy scramblera mogą wygenerować błędną sekwencje bitów, co doprowadzi do utraty synchronizacji,  
- scramblery multiplikatywne są skłonne do błędów podczas descramblingu,  
- scramblery addytywne muszą być resetowane przy użyciu ramki ze synchronizacją (powyżej opisany SYNC). Gdy to nie zadziała wtedy pojawi się poważny błąd przy przesuwaniu bitów, który uniemożliwi descramblerowi rozszyfrowanie sygnału.

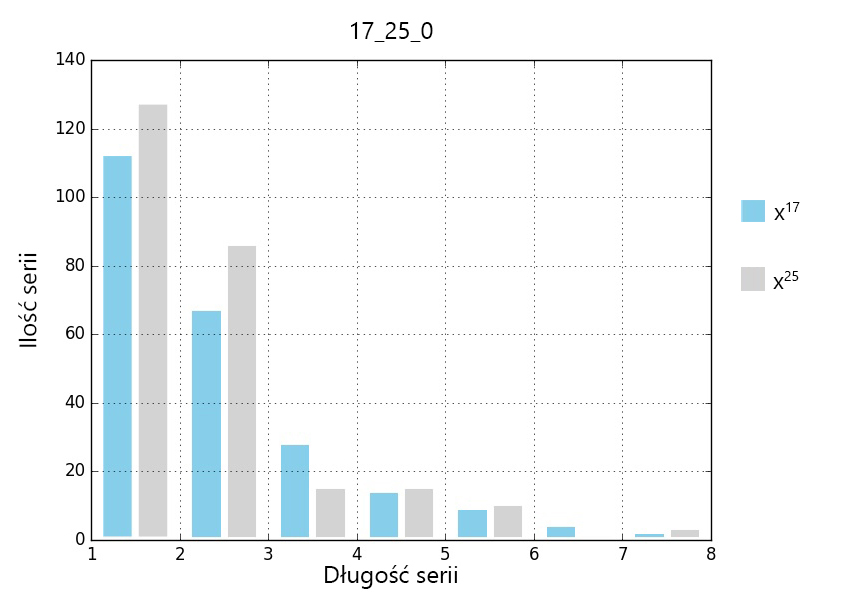
# Wyniki badań

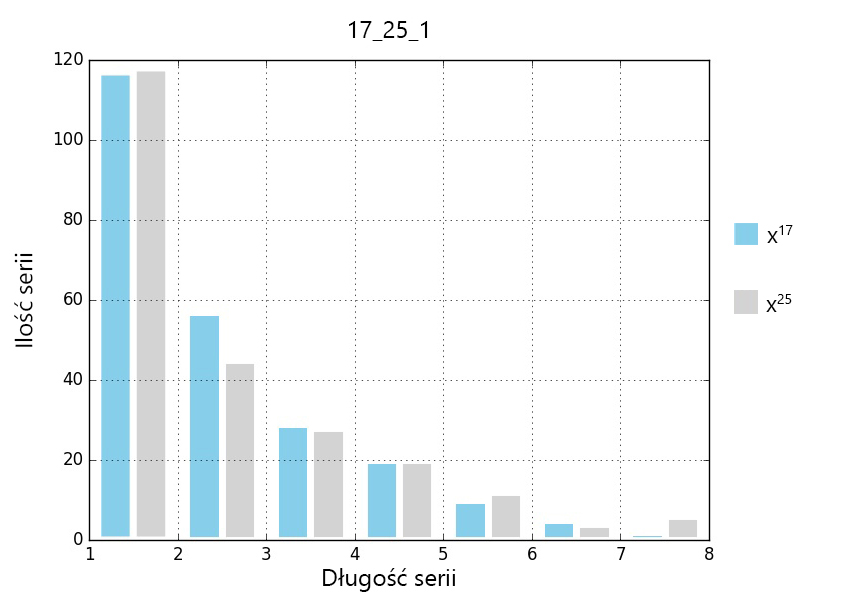
Histogram 1. Wystąpienia ciągów "0" w scramblerach X7 na X43, X7, X43



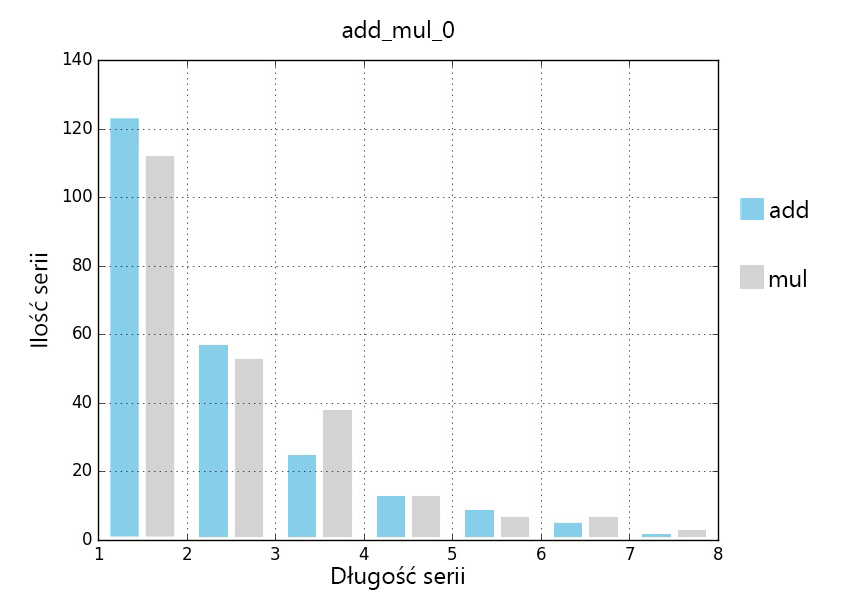
Histogram 2. Wystąpienia ciągów "1" w scramblerach X7 na X43, X7, X43

Histogram 3. Wystąpienia ciągów "0" w scramblerach X17, X25



Histogram 4. Wystąpienia ciągów "1" w scramblerach X17, X25  


Histogram 5. Wystąpienia ciągów "0" w scramblerach DVB i V.34



Histogram 5. Wystąpienia ciągów "1" w scramblerach DVB i V.34

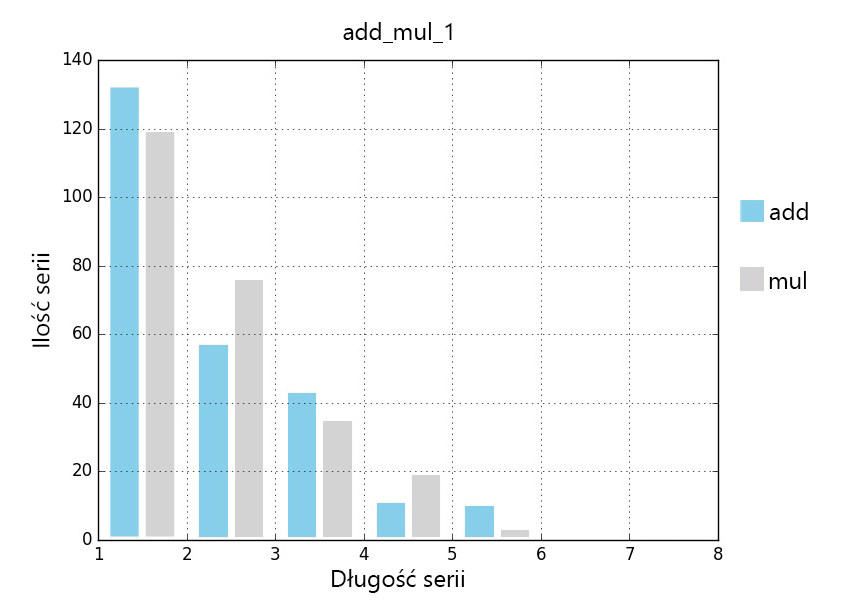


Tabela 1. Średnia długość ciągów "0" i "1" dla [1, 0, 1, 0, 1]

|  |  |  |
| --- | --- | --- |
| **Scrambler** | **Średnia długość ciągów „0”** | **Średnia długość ciągów „1”** |
| DVB | 2.30 | 1.00 |
| V.34 | 1.90 | 2.00 |
| x7+x6+1 | 2.35 | 1.00 |
| x43+1 | 2.00 | 2.00 |
| x7+x6+1 na x43+1 | 2.00 | 2.00 |
| x17+x10+1 | 2.00 | 1.00 |
| x25+1 | 2.00 | 2.00 |

Tabela 2. Średnia długość ciągów "0" i "1" dla [0, 0, 0, 0, 0]

|  |  |  |
| --- | --- | --- |
| **Scrambler** | **Średnia długość ciągów „0”** | **Średnia długość ciągów „1”** |
| DVB | 1.50 | 0.00 |
| V.34 | 1.00 | 2.00 |
| x7+x6+1 | 1.50 | 0.00 |
| x43+1 | 1.00 | 2.00 |
| x7+x6+1 na x43+1 | 2.50 | 2.00 |
| x17+x10+1 | 2.00 | 0.00 |
| x25+1 | 2.00 | 2.00 |

Tabela 3. Średnia długość ciągów "0" i "1" dla [1, 1, 1, 0, 0, …, 0]

|  |  |  |
| --- | --- | --- |
| **Scrambler** | **Średnia długość ciągów „0”** | **Średnia długość ciągów „1”** |
| DVB | 1.50 | 3.00 |
| V.34 | 2.00 | 2.00 |
| x7+x6+1 | 1.50 | 3.00 |
| x43+1 | 2.00 | 1.00 |
| x7+x6+1 na x43+1 | 2.00 | 2.10 |
| x17+x10+1 | 2.10 | 3.00 |
| x25+1 | 1.90 | 1.90 |

Podsumowując wyniki zebrane podczas analizy własności scramblerów oraz podczas pisania kodu programu, jesteśmy w stanie ustalić, zaproponować dwa najlepsze scramblery. Zaproponowane scramblery różnią się jedynie docelowym przeznaczeniem.

*Scrambler x^7+x^6+1* - scrambler ten ma właściwości silnie randomizujące, co pozwala na usunięcie składowej stałej z widma sygnału przesyłanego torami transmisyjnymi; niestety jest również łatwy do złamania z powodu regularnej synchronizacji - jest scramblerem synchronicznym;

*Scrambler x^43+1* – scrambler posiada właściwości silnie szyfrujące, przez co ciężej jest niepowołanej osobie odtworzyć zescramblowany sygnał przesłany torem transmisyjnym; tak samo jak poprzedni scrambler, ten scrambler ma też wady – ma słabe właściwości randomizujące przez co przesyłanie sygnału zajmuje więcej czasu;

# Podsumowanie

Scrambler jest to urządzenie, bez którego nie działałoby wiele rzeczy codziennego użytku, jak na przykład telewizja. Dzięki jego randomizacji bitów nie dopuszczamy do rozsynchronizowania urządzeń. Oczywiście ciągi bitów, czasem są zbyt długie, lecz nasze urządzenie jest synchronizowane dzięki fladze SYNC lub scrambler jest samo-synchronizujący się. Oprócz powyżej wymienionej funkcji scrambler wykorzystuje się do zakodowania informacji, jak na przykład płatna telewizja cyfrowa lub coraz popularniejsze rozwiązania prepaid view.

Descrambler natomiast jest prostym urządzeniem, który za zadanie ma rozkodować sygnał. Urządzenie ma ten sam wielomian, co scrambler, a gdy ktoś zmieni wielomian lub też będzie próbował odczytać zakodowane wiadomości, najprawdopodobniej otrzyma taki sygnał, który będzie niezrozumiały. Dla obrazu będzie to zbiór losowych pikseli, podobnie jak dla filmu, natomiast dla dźwięku nie usłyszymy nic oprócz szumu.