# Implementacja szyfratora strumieniowego, FIPS oraz BBS

Wykonał: Dominik Łukasiewicz, 145290

### 1. BBS:

W pliku "BBS.py" znajduje się skrypt służący do wygenerowania pseudolosowego pliku składającego się z 0 oraz 1.

## Przykładowy wynik programu:



Plik "nisttest.txt" składa się z miliona wygenerowanych liczb 01 przy użyciu BBS. Plik "finalAnalysisReport" przedstawia wyniki z testów wykonanych na oprogramowaniu NIST. Z wyników wynika, że wyłącznie jeden test nie przeszedł.

#### 2. FIPS:

W pliku "BBS.py" znajduje się skrypt służący do przetestowania pliku składającego się z 0 oraz 1. Test FIPS składa się z: single test, series test, long series test oraz poker test.

## Przykładowy wynik programu:

Single test: True Series test: True Long series test: True Poker test: True

# 3. Szyfrator strumieniowy:

W pliku "StreamCipher.py" znajduje się skrypt służący do zaszyfrowania lub deszyfrowania tekstu przy użyciu szyfru strumieniowego.

## Przykładowy plik wejściowy:

```
jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl
```

## **Plik BBS:**

# Plik zaszyfrowany:

# Plik odszyfrowany:

jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl  $jak is\ tekst\ do\ przetestowania\ akldnasobdqwdja; sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl$  $jak is\ tekst\ do\ przetestowania\ akldnasobdqwdja; sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgablugg$  $jak is\ tekst\ do\ przetestowania\ akldnasobdqwdja; sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgablundasbygg$ jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl  $jak is\ tekst\ do\ przetestowania\ akldnasobdqwdja; sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgablugg$ jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl  $jak is\ tekst\ do\ przetestowania\ akldnasobdqwdja; sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgablugandur. The proposed state of the proposed sta$ jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl jakis tekst do przetestowania akldnasobdqwdja;sdasfbqwasldaodfbaldknaslfjgwuhawlisasfbsdfjksdfasldkasncljdzfbalsffbafgabl