**Sprawozdanie**

*Bezpieczeństwo Sieci Komputerowych*

Pracownia Specjalistyczna 4-5



Temat:   
**GENERATORY LICZB PSEUDOLOSOWYCH. SZYFRY STRUMIENIOWE.**

Wykonanie:

**Busłowski Tomasz**

**Suchwałko Tomasz**

Prowadzący zajęcia: **dr inż. Maciej Brzozowski**

**Zadania do wykonania:**

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

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

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

**Środowisko, framework i język implementacji zadań:**

* Microsoft Visual Studio Enterprise 2015 (Version 14.0.25431.01 Update 3).
* Microsoft .NET Framework (Version 4.6.01586).
* C# 6.0.

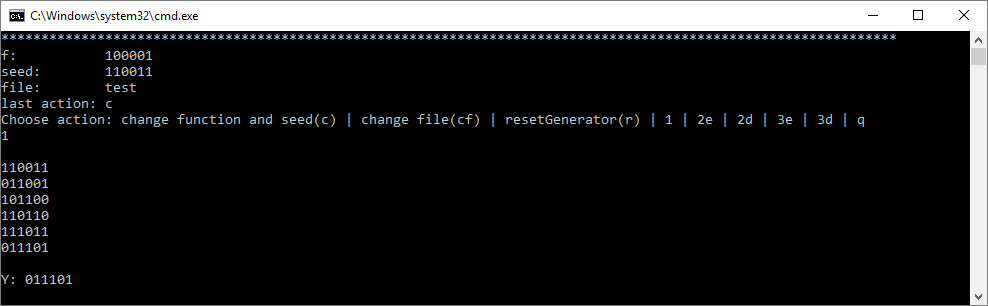
**Wykonanie zadań:**

Wszystkie zadania zostały wykonane.

* Tomasz Busłowski – 1, 2
* Tomasz Suchwałko – 2, 3

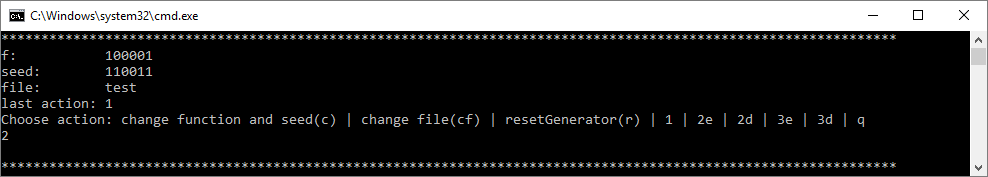
**Screeny wykonanych zadań:**

1. Generator liczb pseudolosowych bazujący na LFSR o zadanym stopniu wielomianu:

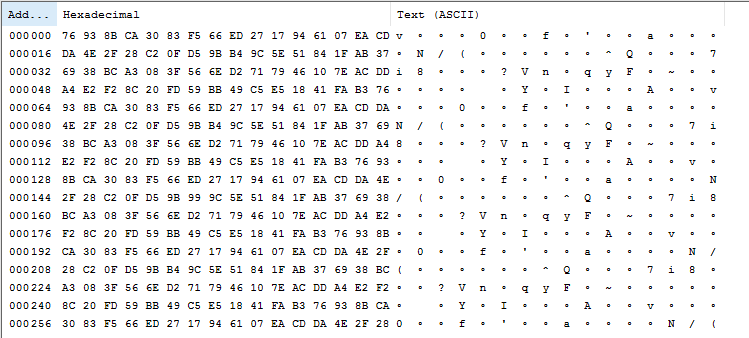


Rysunek 1

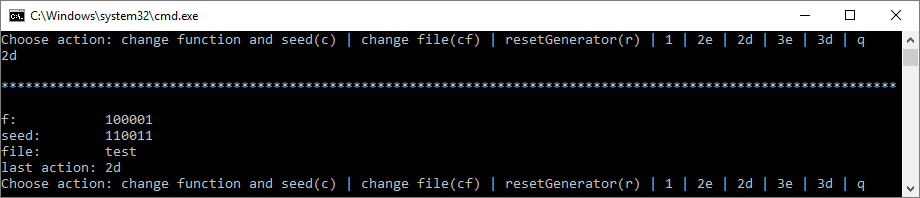
1. Kryptosystem bazujący na schemacie Synchronous Stream Cipher dla podanego wielomianu i ziarna:



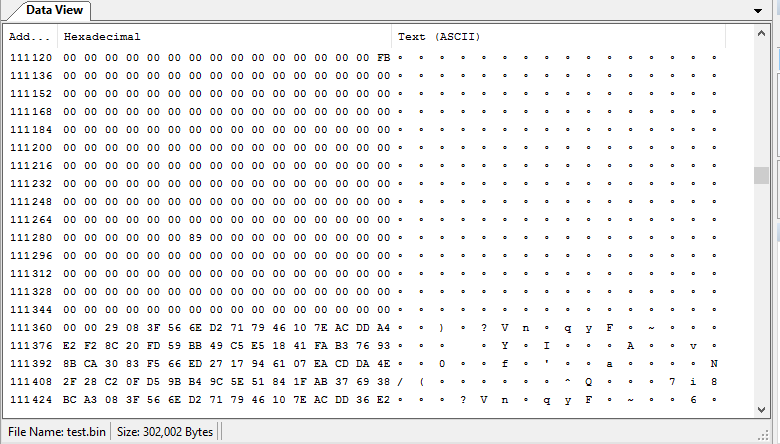
Rysunek 2 - wykonanie kodowania



Rysunek 3 - zakodowany plik

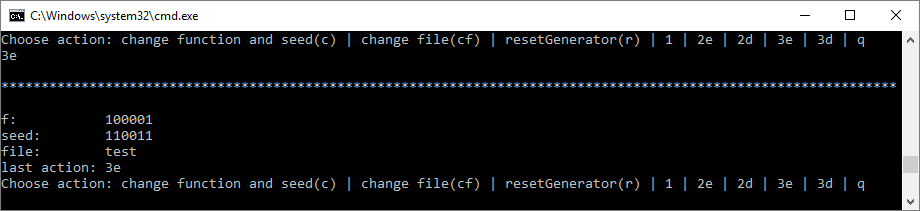


Rysunek 4 - wykonanie dekodowania

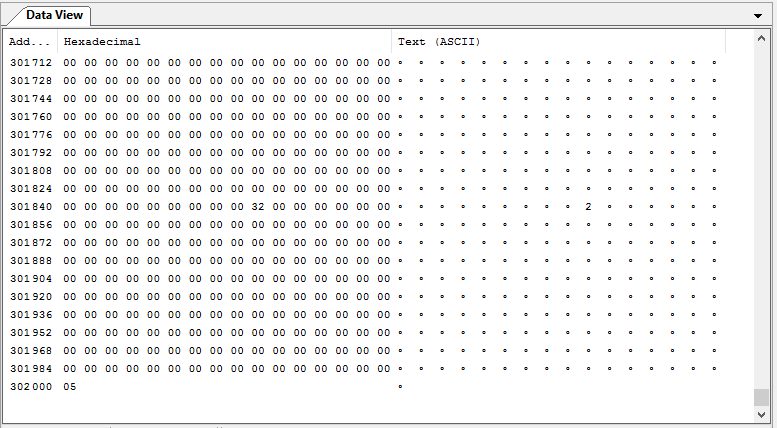


Rysunek 5 - odkodowany plik do którego w połowie wstawiliśmy 'x' – od połowy pliku widać krzaki

1. Kryptosystem bazujący na schemacie Ciphertext Autokey dla podanego wielomianu i ziarna.



Rysunek 6 - wykonanie kodowania



Rysunek 7 - Po wstawieniu "x" w środku zaszyfrowanego pliku, przy odkodowywaniu, został dopisany dodatkowy bajt