

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**

BSK, semestr VI, 21-03-2017, Wydział Informatyki, Politechnika Białostocka

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.

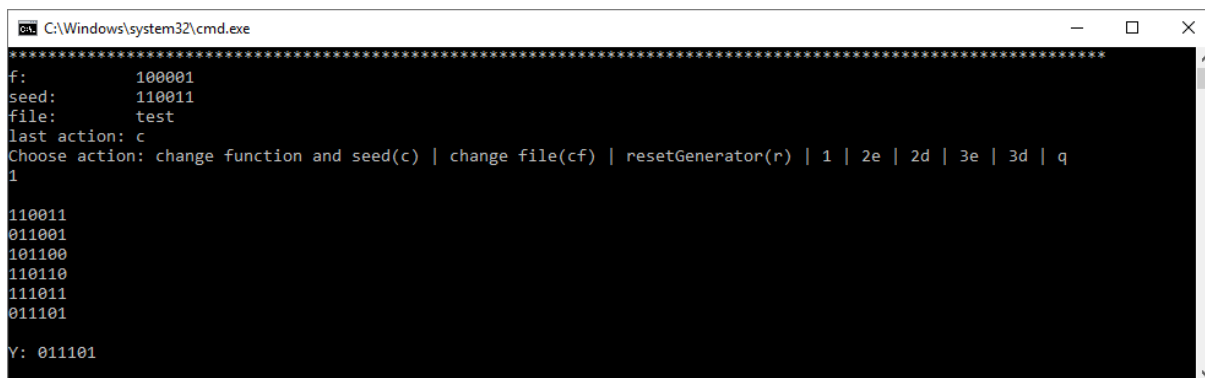
Wykonanie zadań:

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:



```
C:\Windows\system32\cmd.exe
*****
f:      100001
seed:   110011
file:   test
last action: c
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q
1
110011
011001
101100
110110
111011
011101
Y: 011101
```

Rysunek 1

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

```

C:\Windows\system32\cmd.exe
*****
f:      100001
seed:   110011
file:   test
last action: 1
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q
2
*****

```

Rysunek 2 - wykonanie kodowania

Add...	Hexadecimal	Text (ASCII)
000000	76 93 8B CA 30 83 F5 66 ED 27 17 94 61 07 EA CD v	0 f ' a
000016	DA 4E 2F 28 C2 0F D5 9B B4 9C 5E 51 84 1F AB 37	N / (^ Q 7
000032	69 38 BC A3 08 3F 56 6E D2 71 79 46 10 7E AC DD i	8 ? V n q y F ~
000048	A4 E2 F2 8C 20 FD 59 BB 49 C5 E5 18 41 FA B3 76	Y I A v
000064	93 8B CA 30 83 F5 66 ED 27 17 94 61 07 EA CD DA	0 f ' a
000080	4E 2F 28 C2 0F D5 9B B4 9C 5E 51 84 1F AB 37 69 N	/ (^ Q 7 i
000096	38 BC A3 08 3F 56 6E D2 71 79 46 10 7E AC DD A4 8	? V n q y F ~
000112	E2 F2 8C 20 FD 59 BB 49 C5 E5 18 41 FA B3 76 93	Y I A v
000128	8B CA 30 83 F5 66 ED 27 17 94 61 07 EA CD DA 4E	0 f ' a N
000144	2F 28 C2 0F D5 9B 99 9C 5E 51 84 1F AB 37 69 38 /	(^ Q 7 i 8
000160	BC A3 08 3F 56 6E D2 71 79 46 10 7E AC DD A4 E2	? V n q y F ~
000176	F2 8C 20 FD 59 BB 49 C5 E5 18 41 FA B3 76 93 8B	Y I A v
000192	CA 30 83 F5 66 ED 27 17 94 61 07 EA CD DA 4E 2F	0 f ' a N /
000208	28 C2 0F D5 9B B4 9C 5E 51 84 1F AB 37 69 38 BC	(^ Q 7 i 8
000224	A3 08 3F 56 6E D2 71 79 46 10 7E AC DD A4 E2 F2	? V n q y F ~
000240	8C 20 FD 59 BB 49 C5 E5 18 41 FA B3 76 93 8B CA	Y I A v
000256	30 83 F5 66 ED 27 17 94 61 07 EA CD DA 4E 2F 28 0	0 f ' a N /

Rysunek 3 - zakodowany plik

```

C:\Windows\system32\cmd.exe
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q
2d
*****
f:      100001
seed:   110011
file:   test
last action: 2d
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q

```

Rysunek 4 - wykonanie dekodowania

Data View		
Add...	Hexadecimal	Text (ASCII)
111120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FB	• • • • • • • • • • • • • • • •
111136	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111152	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111168	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111184	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111216	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111248	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111264	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111280	00 00 00 00 00 00 00 89 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111296	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111312	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111328	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111344	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	• • • • • • • • • • • • • • • •
111360	00 00 29 08 3F 56 6E D2 71 79 46 10 7E AC DD A4	• • • • • • • • • • • • • • • •
111376	E2 F2 8C 20 FD 59 BB 49 C5 E5 18 41 FA B3 76 93	• • • • • • • • • • • • • • • •
111392	8B CA 30 83 F5 66 ED 27 17 94 61 07 EA CD DA 4E	• • • • • • • • • • • • • • • •
111408	2F 28 C2 0F D5 9B B4 9C 5E 51 84 1F AB 37 69 38	/ (• • • • • • • • • • • • • •
111424	BC A3 08 3F 56 6E D2 71 79 46 10 7E AC DD 36 E2	• • • • • • • • • • • • • • • •

File Name: test.bin | Size: 302,002 Bytes

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

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

```

C:\Windows\system32\cmd.exe
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q |
3e

*****

f:      100001
seed:   110011
file:    test
last action: 3e
Choose action: change function and seed(c) | change file(cf) | resetGenerator(r) | 1 | 2e | 2d | 3e | 3d | q

```

Rysunek 6 - wykonanie kodowania

Add...	Hexadecimal	Text (ASCII)
301712	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301728	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301744	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301760	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301776	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301792	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301808	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301824	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301840	00 00 00 00 00 00 00 00 00 00 32 00 00 00 00 00 2
301856	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301872	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301888	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301904	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301920	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301936	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301952	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301968	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
301984	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
302000	05	.

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