УДК 004.056.55, УДК 004.421.5

О.В. ГРЕСЬ, М.І. СКРИПСЬКИЙ
Чернівецький національний університет імені Юрія Федьковича
В.М. КОСОВАН
Чернівецький ліцей № 1
Г.М. РОЗОРІНОВ
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ДИСКРЕТНИХ ВІДОБРАЖЕНЬ

Досліджені генератори псевдовипадкових послідовностей на основі дискретних відображень. Тестування статистичних властивостей проводилось з використанням пакету тестів NIST STS 2.1.2. Запропонований генератор псевдовипадкових послідовностей на основі комбінації лінійного конгруентного генератора та генератора на основі логістичного відображення для якого встановлено діапазон значень параметру керування λ при якому послідовності, генеровані запропонованим генератором задовольняють вимогам статистичних тестів. Проведені дослідження чутливості та криптостійкості генераторів псевдовипадкових послідовностей на основі дискретних відображень.

Ключові слова: генератор, логістичне відображення, псевдовипадкова послідовність, статистичні тести, криптостійкість.

O.V. HRES, M.I. SKRYPSKYJ
Yuriy Fedkovych Chernivtsi National University
V.M. KOSOVAN
Chernivtsi Lyceum №1
G.M. ROZORYNOV
Natoinal Technical
University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

THE RESEARCH OF GENERATORS OF PSEUDORANDOM SEQUENCES BASED ON DISCRETE MAPPINGS

We study the generators of pseudorandom sequences based on discrete mappings. Testing of statistical properties was performed using the NIST STS 2.1.2 test package. The proposed pseudorandom sequence generator based on a combination of a linear congruent generator and a generator based on logistic mapping for which a range of values of the control parameter λ is established for which the sequence generated by the proposed generator satisfies the requirements of statistical tests. The investigates of sensitivity and cryptography stability of pseudorandom sequence generators on the based of discrete mappings. To investigate the statistical priorities of generators used test NIST STS 2.1.2. From the results of research generator set, generator based on a combination of linear congruent generator and generator based on logistic map satisfies the requirements of cryptographic tests at values control parameters $\lambda \in [3,97; 4]$, while the generator based on logistic map that value is within $\lambda \in [3.99\ 4]$. Research on the cryptography stability of input parameters was conducted using the "brute force" attack. Analysis of the cryptography stability of generators showed that exhaustive search for clues at management settings setting accuracy of 11 decimal places must be expended under control parameter values $\lambda \in [3,99; 4]$, while the values of $\lambda \in [3,97; 4]$ time costs amount to 9,5 years.

Keywords: generator, logistic mapping, pseudo-random sequence, statistical tests, cryptography stability.

Вступ

В останні роки бурхливим розвитком телекомунікаційних систем, інтернет технологій, IP-телефонії постала проблема захисту інформації, що передається по цифровим каналам зв'язку через мережу Internet/Ethernet. Сучасні інформаційні системи вимагають забезпечення високої скритності і конфіденційності зв'язку. Захист інформації, яка передається в таких системах можливий шляхом її шифрування за допомогою криптостійких бінарних послідовностей [1–3].

Генерування криптостійких бінарних послідовностей є на сьогоднішній день актуальною задачею. Генератори ключових послідовностей є невід'ємними і важливими елементами будь-яких криптографічних додатків. На даний час відомі алгоритми генерування криптостійких бінарних послідовностей на основі еліптичних кривих, клітинних автоматів, теорії детермінованого хаосу [1–3].

Основною особливістю генераторів бінарних послідовностей, алгоритми генерування яких реалізовані на основі теорії детермінованого хаосу, є висока чутливість до зміни початкових умов [1–3].

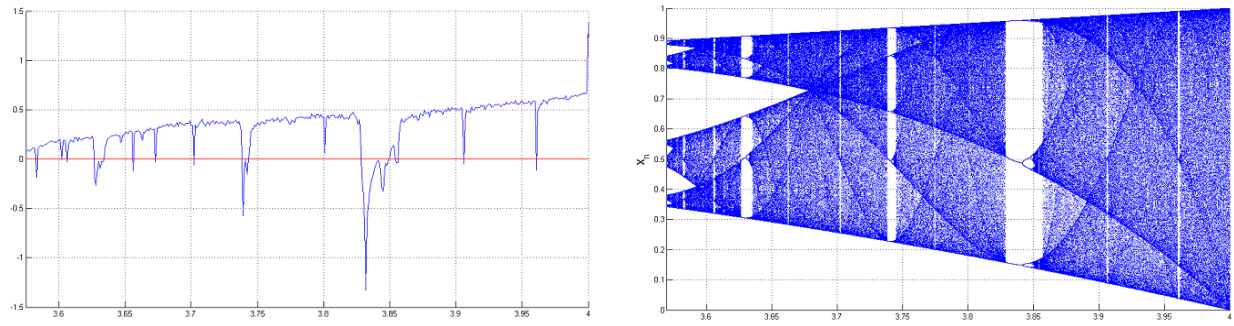
Дослідження статистичних характеристик генератора бінарних послідовностей на основі логістичного відображення

Генерування цифрових хаотичних послідовностей здійснюється з використанням певної аналітичної функції, значення якої за певних початкових умовах рівномірно розподілені на обмеженому інтервалі. Такою властивістю володіють розв'язки логістичного рівняння, що описується формулою (1):

$$x_{n+1} = \lambda \cdot x_n (1 - x_n), \tag{1}$$

де λ – параметр, x_0 – початкова умова для генерування послідовностей.

Залежно від значення λ генеровані коливання можуть бути періодичними, квазіперіодичними або хаотичними [4,5].

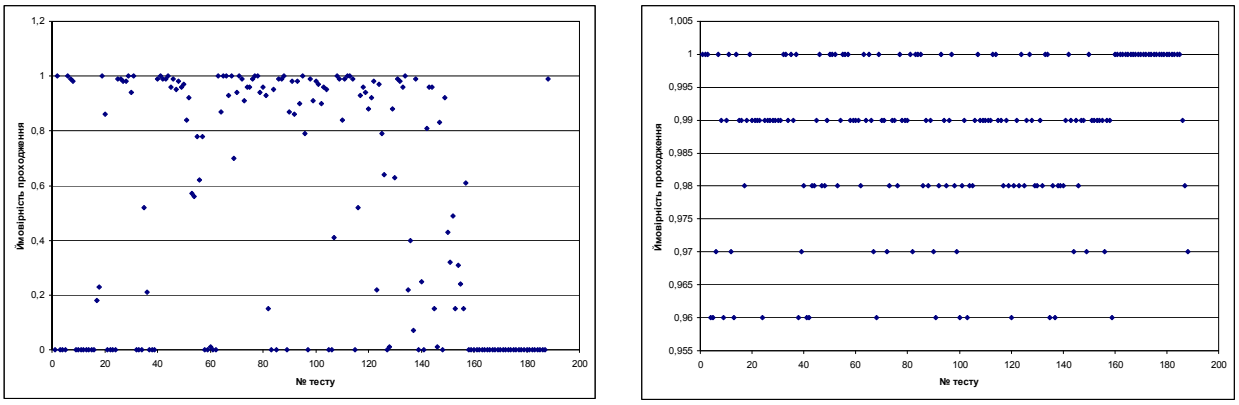


а б

Рис. 1. Показник Ляпунова для логістичного відображення при значеннях $\lambda \in$ [3,56;4] а) та біфуркаційна діаграма для значень $\lambda \in$ [3,56;4] б) відповідно

Із залежностей показника Ляпунова від параметру керування λ (рис.1а) та біфуркаційної діаграми (рис. 1б) логістичного відображення випливає, що при $\lambda \geq 3{,}56$ показник Ляпунова набуває додатніх значень, а біфуркація подвоєння періоду має велику частоту, що і вказує на хаотичну природу коливань [4,5].

Проведемо дослідження генератора псевдовипадкових послідовностей на базі логістичного відображення, що може використовуватись в методах потокового шифрування інформації як генератор ключових послідовностей [3–5]. Для цього використаємо пакет статистичних тестів NIST STS 2.1.2. при значеннях параметру керування $\lambda \in$ [3,56;4]. Тестуванню підлягали 10^3 послідовностей довжиною $m=10^6$ бітів кожна, таким чином досліджуваний масив становить 10^9 бітів. Для детального аналізу було проведено тестування генератора при різних значеннях параметру керування $\lambda \in$ [3,56;4]. Побудовані за результатами тестування статистичні портрети генератора, приведені на рис. 2 а та 2 б, відповідно.



а б

Рис. 2. Статистичний портрет генератора на основі логістичного відображення
а - при значеннях параметру керування λ=3,78 та початковій умові x_0=0,5;
б - при значеннях параметру керування λ=3,99 та початковій умові x_0=0,5

Із отриманих результатів випливає, що при зміні параметра керування в межах $\lambda \in$ [3,56;4], кількість тестів, за якими випробування є незадовільними зменшується, тобто якість генерованих послідовностей з точки зору випадковості покращується. Зокрема, при значеннях параметру λ=3,99 та початкової умови x_0=0,5 більшість тестів пройдено на рівні більше 0,96, що вказує на псевдовипадковий характер генерованих послідовностей. За результатами досліджень можна зробити висновок, що значення параметру керування λ, при яких даний генератор задовольняє вимогам криптографічних тестів, знаходиться в діапазоні $\lambda \in$ [3,99;4] [4,5].

Таблиця 1

Результати проходження тестів NIST генератором на основі логістичного відображення (при значеннях параметру керування λ=3,99 та початковій умові x_0=0,5) та генераторами BBS та ANSI (3-DES)

Генератор	Кількість тестів, пройдених більше 99% послідовностей	Кількість тестів, пройдених більше 96% послідовностей
Генератор BBS	134 (71,3%)	188 (100%)
Генератор ANSI X9.17 (3-DES)	121 (64,4%)	188 (100%)
Генератор на основі логістичного відображення	128 (68,1%)	188 (100%)

У таблиці 1 приведені результати порівняння властивостей послідовностей, генерованих на основі логістичного відображення із властивостями псевдовипадкових послідовностей (ПВП), сформованими генераторами BBS та ANSI X9.17 (3-DES) (тестова вибірка, рекомендована NIST) [10].

Із отриманих практичних результатів випливає, що генеровані за логістичним дискретним відображенням ПВП мають задовільні статистичні характеристики в діапазоні значень параметру керування $\lambda \in [3,99;4]$. Отже, недоліком даного генератора є обмеженість діапазону параметру керування для генерування ПВП. Тому більш ефективним методом для генерування криптостійких ПВП буде використання комбінації генераторів.

Дослідження статистичних характеристик генератора бінарних послідовностей з нормальним розподілом значень їх елементів

Блок-схема генератора псевдовипадкових послідовностей з нормальним розподілом значень їх елементів приведена на рис. 3.

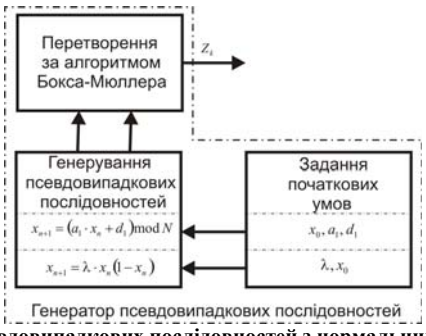


Рис. 3. Блок-схема генератора псевдовипадкових послідовностей з нормальним розподілом значень їх елементів

Робота генератора базується на основі двох генераторів псевдовипадкових послідовностей, які працюють з різними початковими умовами, генератора на основі логістичного відображення (1) та лінійного конгруентного генератора (2) [6-8]:

$$x_{n+1} = (a_1 \cdot x_n + d_1) \bmod N, \tag{2}$$

де *a, d, N* – константи. При проведенні досліджень вибиралися наступні значення параметрів: для лінійного конгруентного генератора такі, що забезпечують максимальне значення періоду повторень (наприклад $a = 7^5 = 16807$, $d = 7$ та $N = 2^{31}-1 = 2147483647$), а для логістичного відображення значення початкової умови та параметру керування становили $x_0 = 0,5$ та $\lambda \in [3,56;4]$ відповідно.

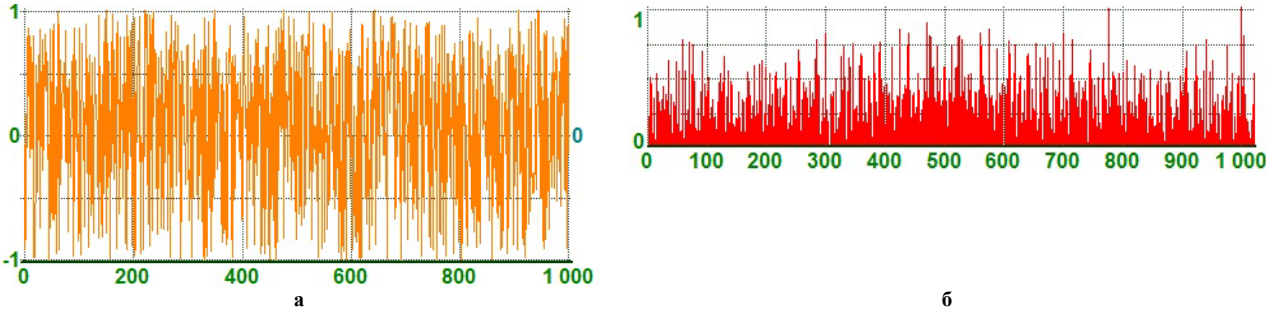
Вихідні послідовності цих генераторів перетворюються за допомогою алгоритму Бокса-Мюллера [7–9] в послідовність псевдовипадкових дійсних чисел, що належать інтервалу [-1;1], розподілених за законом Гауса згідно наступних співвідношень:

$$\nu = x_1^2 + x_2^2, \tag{3}$$

$$z_1 = x_1 \cdot \sqrt{\frac{-2\log(\nu)}{\nu}}, \quad z_2 = x_2 \cdot \sqrt{\frac{-2\log(\nu)}{\nu}}, \tag{4}$$

де x_1, x_2 два числа, отримані від генераторів псевдовипадкових чисел, а y_1, y_2 – два псевдовипадкових нормально розподілених числа. Якщо при цьому сума квадратів чисел x_1 та x_2 є більшою за 1, тобто $\nu = x_1^2 + x_2^2$, то даний результат приймається та вибирається наступне випадкове число.

Програмна реалізація даного генератора здійснювалась на мові програмування Delphi 7. Вигляд генерованої послідовності та її спектральне представлення показані на рис. 4 а та 4 б, відповідно.



а **б**

Рис. 4. Вигляд послідовності, сформованої генератором псевдовипадкових послідовностей з нормальним розподілом значень їх елементів а - часове представлення послідовності, б - спектральне представлення послідовності

Дослідження запропонованого генератора ПВП з нормальним розподілом проводилось з використанням статистичних тестів NIST STS 2.1.2. Для тестування було обрано 10^3 послідовностей довжиною $m=10^6$ бітів кожна, таким чином досліджуваний масив становить 10^9 бітів.

Для детального аналізу було проведено тестування генератора при різних значеннях параметру керування $\lambda \in [3,56;4]$. Побудовані за результатами тестування статистичні портрети генератора, приведені

на рис. 5.

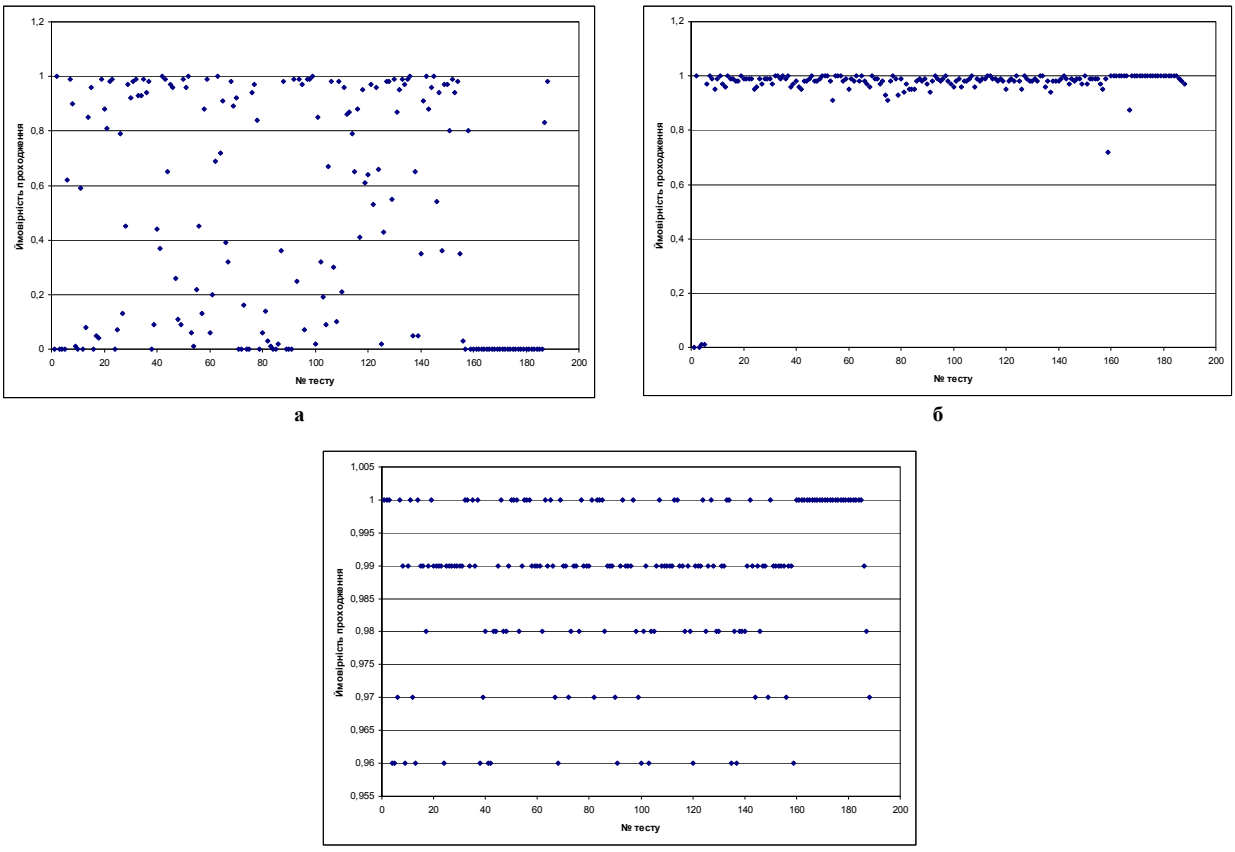


Рис. 5. Статистичні портрети генератора псевдовипадкових послідовностей з нормальним розподілом їх значень при значенні початкової умови x_0=0,5 та значеннях параметру керування: а - λ=3,78; б - λ=3,92; в - λ=3,975

Із отриманих результатів випливає, що при зміні параметра керування в межах $\lambda \in [3,56;4]$, кількість тестів, за якими випробування є незадовільними зменшується, тобто якість генерованих послідовностей з точки зору випадковості покращується. Зокрема, при значеннях параметру λ=3,97 та початкової умови x_0=0,5 більшість тестів пройдено на рівні більше 0,96, що вказує на псевдовипадковий характер генерованих послідовностей (на рис. 5в зображений статистичний портрет при одному з випадків, зокрема при λ=3,975). За результатами досліджень можна зробити висновок, що значення параметру λ при яких даний генератор задовольняє вимогам криптографічних тестів знаходиться в діапазоні $\lambda \in [3,97;4]$ [5,6].

В таблиці 2 приведені результати порівняння властивостей ПВП, генерованих запропонованим генератором з нормальним розподілом (при одному із значень параметру керування, зокрема при λ=3,975) із генератором псевдовипадкових бітів BBS та генератором ANSI X9.17 (3-DES) (тестова вибірка, рекомендована NIST) (тестова вибірка, рекомендована NIST).

Таблиця 2

Результати проходження тестів NIST генератором з нормальним розподілом (при значеннях параметру керування λ=3,975 та початковій умові x_0=0,5) та генераторами BBS та ANSI (3-DES)

Генератор	Кількість тестів пройдених більше 99% послідовностей	Кількість тестів пройдених більше 96% послідовностей
Генератор BBS	134 (71,3%)	188 (100%)
Генератор ANSI X9.17 (3-DES)	121 (64,4%)	188 (100%)
Генератор з нормальним розподілом	132 (70,2%)	188 (100%)

З результатів дослідження генераторів встановлено, що генератор на основі комбінації лінійного конгруентного генератора та генератора на основі логістичного відображення задовольняє вимогам криптографічних тестів при значеннях параметру керування $\lambda \in [3,97;4]$., тоді як для генератора на основі логістичного відображення це значення знаходиться в межах [3,99;4]. Отже, при використанні комбінації генераторів для генерування ПВП потужність простору ключів зростає.

Вцілому, із проведених результатів досліджень випливає, що вище наведені генератори ПВП на основі дискретних відображень мають задовільні статистичні характеристики, а генеровані бітові послідовності задовольняють вимогам статистичних тестів NIST, тобто їх можна вважати статистично

безпечними.

Дослідження криптостійкості дискретних відображень за вхідними параметрами

Дослідження криптостійкості за вхідними параметрами проведемо з використанням атаки "груба сила". Атака "груба сила" [10] типу перебирання ключів описується кількістю варіантів (команд) що необхідно виконати для встановлення ключа (дешифрувати його). Основним показником методу перебору є кількість варіантів перебирання та час перебирання [10]:

Ключем для генерування послідовностей шифрування з використанням логістичного відображення є значення параметра керування λ і початкове значення x_0. При цьому кількість ключів для генерування послідовностей визначатиметься за наступною формулою:

$$N = (10^n)^2 \tag{5}$$

де n - точність завдання параметрів (кількість знаків після коми).

У нашому випадку точність введення n для λ і x_0 задаватиметься із точністю до десятого знаку (мінімально), що відповідає потужності простору ключів $(10^{10})^2 = 10^{20}$, а час перебору ключів становитиме [10]:

$$t = \frac{N_K}{\gamma \cdot K} P_P, \tag{6}$$

де N_K – число ключів, що можуть використовуватись в системі, γ – потужність криптоаналітичної системи; P_P – ймовірність успішного криптоаналізу; K =3,15x10^7 – кількість секунд у році, t – час повного перебору в роках.

Враховуючи, що потужність криптоаналітичної системи становить $\gamma = 10^{11}$ -10^{12} комбінацій за секунду, матимемо:

$$t = \frac{10^{20}}{10^{12} \cdot 3{,}15 \cdot 10^7} = 3{,}17$$

Отже перебір варіантів при заданій точності займе 3,17 років.

В таблиці 3 приведені часові витрати необхідні для перебору всіх можливих комбінацій в залежності від точності представлення початкових умов для генератора на основі логістичного відображення та комбінації генераторів (логістичного та лінійного конгруентного)

Таблиця 3

Часові затрати для повного перебору значень параметру керування в межах λ∈ [3,97;4] при кроці 0,01 (для генератора бінарних послідовностей на основі логістичного відображення та на основі комбінації лінійного конгруентного генератора логістичного відображення)

Точність представлення значень параметрів (кількість знаків після коми)	Діапазон значень параметру керування	Простір ключів	Необхідні часові витрати для повного перебору значень вхідних параметрів (в роках)
10	λ =[3,97;4]	$0{,}03 \cdot 10^{20}$	0,095
11	λ =[3,97;4]	$0{,}03 \cdot 10^{22}$	9,52
12	λ =[3,97;4]	$0{,}03 \cdot 10^{24}$	952,3
10	λ =[3,98;4]	$0{,}02 \cdot 10^{20}$	0,063
11	λ =[3,98;4]	$0{,}02 \cdot 10^{22}$	6,34
12	λ =[3,98;4]	$0{,}02 \cdot 10^{24}$	634,92
10	λ =[3,99;4]	$0{,}01 \cdot 10^{20}$	0,0317
11	λ =[3,99;4]	$0{,}01 \cdot 10^{22}$	3,174
12	λ =[3,99;4]	$0{,}01 \cdot 10^{24}$	317,4

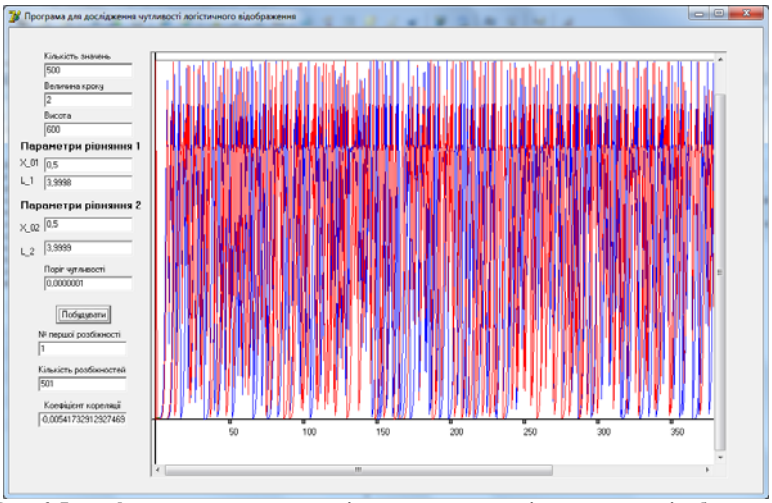


Рис. 6. Інтерфейс програми для дослідження чутливості дискретних відображень

Аналіз криптостійкості генераторів показав, що для повного перебору ключів при точності завдання параметрів керування в 11 знаків після коми необхідно затратити 3,2 років при значеннях параметра керування $\lambda \in [3{,}99;4]$, а при значеннях $\lambda \in [3{,}97;4]$ часові затрати становитимуть 9,5 років.

Дослідження чутливості та кореляції дискретних відображень

Проведемо дослідження логістичного відображення на чутливість по параметру керування λ. Для дослідження чутливості генераторів по вхідним параметрам на мові програмування Delphi 7 було розроблено програмне забезпечення, інтерфейс якого наведений на рис. 6.

Програма дозволяє задавати початкові умови та параметри для 2-х рівнянь: ($x_{(n+1)} = \lambda x_n (1 - x_n)$ – перше рівняння, $y_{(n+1)} = \lambda y_n (1 - y_n)$ – друге рівняння, а також встановлювати поріг чутливості (якщо різниця між значеннями двох рівнянь $x_{(n+1)} - y_{(n+1)}$ більша за даний поріг, то такі значення будуть рахуватись розбіжностями). Для дослідження було обрано 500 значень генерованих послідовностей. За отриманими результатами досліджень було побудовано графіки залежності кількості та номеру першої розбіжності від різниці між значеннями параметрів при різних порогах чутливості, які наведені на рис. 7 та 8, відповідно.

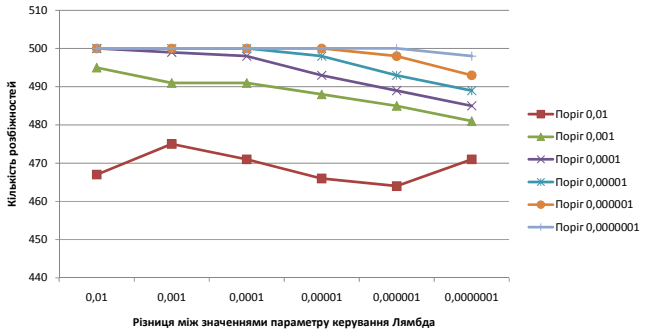


Рис. 7. Залежність кількості розбіжності значень від різниці значень параметрів керування логістичного відображення

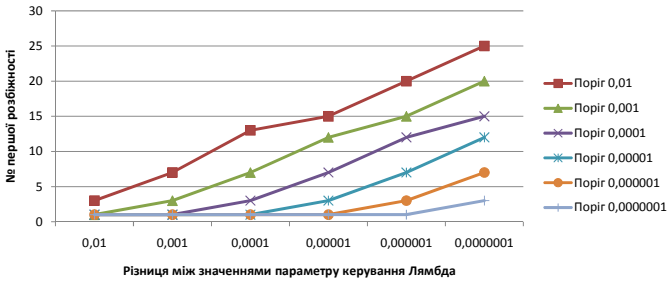


Рис. 8. Залежність номера розбіжності значень від різниці значень параметрів керування логістичного відображення

З проведених досліджень встановлено, що розбіжності в значеннях функції з'являються вже при зміні параметра керування на 0,0000001 при порозі розбіжності 0,0000001

Для більш якісного аналізу проведемо дослідження коефіцієнту кореляції між значеннями функцій $x_{(n+1)}$ та $y_{(n+1)}$. Коефіцієнт кореляції обчислюється за формулою [7–9, 11, 12]:

$$C_p = \frac{N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{N\left\{\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right\}}\sqrt{N\left\{\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right\}}}, \quad (7)$$

де x, y, j, i – значення генерованих послідовностей,

N – значень послідовностей, вибраних для розрахунку коефіцієнту кореляції.

Для розрахунку коефіцієнту кореляції було обрано 500 значень генерованих послідовностей. Дослідження проводилось при наступних значеннях параметрів: $x_0 = y_0 = 0{,}5$; $\lambda_1 = 3{,}9999999999$, $\lambda_2 = 3{,}9999999998$ (графік 1) та $\lambda_1 = \lambda_2 = 3{,}9999999999$; $x_0 = 0{,}5$; $y_0 = 0{,}499999999$ (графік 2). Залежність коефіцієнта кореляції від кількості значень генерованих послідовностей показана на рис. 9.

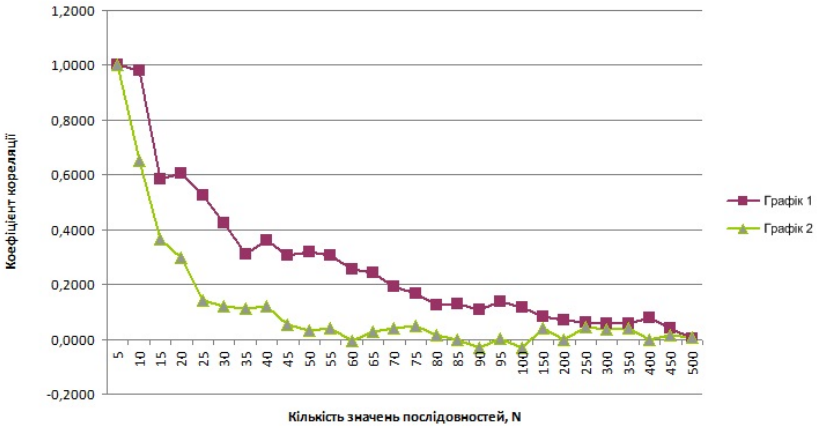


Рис. 9. Графік залежності коефіцієнта кореляції ПВП від кількості генерованих значень

З отриманих результатів можна зробити висновок, що найкращі властивості мають значення послідовностей починаючи з *N*-100 значень.

Застосування генераторів ПВП на основі дискретних відображень у схемах шифрування інформації

На основі розроблених генераторів ПВП та методів кодування інформації нами запропонована система кодування/декодування інформації з її додатковим шифруванням елементами хаотичної послідовності, генерованої на основі дискретних відображень [13]. Система складається з наступних блоків: блок кодування/декодування, блок шифрування/розшифрування, генератор ПВП, блок завдання початкових умов. Структурна схема системи кодування/декодування інформації з її додатковим шифруванням показана на рис. 10.

Запропонована система використовує метод адаптивного арифметичного стиснення з додатковим потоковим шифруванням стиснутої інформації псевдовипадковими послідовностями. Як блок кодування використовується двійковий адаптивний арифметичний кодер.

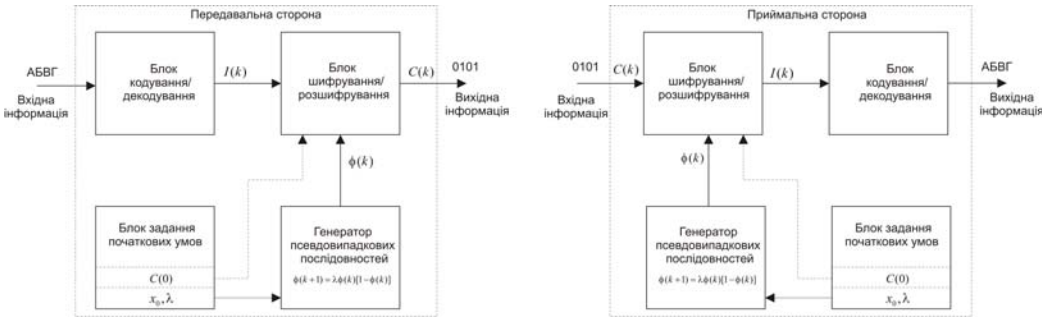


Рис. 10. Структурна схема системи кодування/декодування з додатковим шифруванням

Блоки системи можуть бути реалізовані з використанням апаратно-програмних модулів. Робота системи досліджувалась на прикладі кодування текстової інформації.

Система працює наступним чином. Інформація, що поступає на вхід системи (блоку кодування) на передавальній стороні, кодується та стискується за алгоритмом адаптивного арифметичного кодування, внаслідок чого формується двійкова послідовність (I), що представляє закодовану інформацію. Далі, закодована інформація надходить на вхід блоку шифрування, в якому зашифровується елементами псевдовипадкової послідовності, генерованої на основі логістичного відображення. В якості методу шифрування використовується модифіковане перетворення дифузії, запропоноване в [9]. Дане перетворення зв'язує значення поточних закодованих байтів інформації (тексту) (I_k) з наступними байтами інформації (тексту), отриманими після шифрування (C_k). Механізм дифузії описується наступною формулою:

$$C(k) = \phi(k) \oplus \{[I(k) + \phi(k)] \bmod N\} \oplus I(k-1), \quad (8)$$

де C(k) – байти зашифрованої інформації (тексту), $I(k)$ – байт інформації (тексту), отриманої після стиснення; $I(k-1)$ – попередній байт інформації (тексту), отриманої після стиснення (з виходу блоку кодування) (при k=1 замість $I(k-1)$ беремо відповідне задане нами значення C(0), яке, зокрема, можна вважати додатковим ключем шифрування), $\phi(k)$ – байти псевдовипадкової послідовності, генерованої на основі логістичного відображення:

$$\phi(k+1) = \lambda\phi(k)[1-\phi(k)]. \quad (9)$$

Обернене перетворення дифузії (3.12) перепишеться у наступному вигляді:

$$I(k) = \{\phi(k) \oplus C(k) \oplus I(k-1) + N - \phi(k)\} \bmod N. \quad (10)$$

Таким чином, на виході системи утворюється стиснуте двійкове кодове повідомлення (С), що додатково зашифроване псевдовипадковими послідовностями. Додаткове шифрування унеможливлює розшифрування інформації, якщо не відомий ключ для запуску генератора псевдовипадкової послідовності. Як ключ для генератора на основі логістичного відображення виступають наступні параметри: початкова умова ϕ_0 та значення параметру керування λ (в нашому випадку $\lambda = 3{,}99$). На приймальній стороні розшифрування та декодування інформації здійснюється у зворотному порядку. Для синхронізації передавальної та приймальної сторін системи можна використати спосіб синхронізації, запропонований в [14].

Запропонована система була реалізована на програмному рівні. В таблиці 4 приведений порівняльний аналіз систем кодування інформації з додатковим її шифруванням на основі дискретних відображень.

Таблиця 4

Порівняльний аналіз систем кодування інформації з додатковим шифруванням

Початковий розмір файлу, Кб	Система кодування інформації з додатковим шифруванням в [15,16]		Розроблена система арифметичного кодування з додатковим шифруванням	
	Час кодування, мс	Час декодування, мс	Час кодування, мс	Час декодування, мс
1396	590	631	540	587
1403	560	601	512	565
1428	480	501	443	492

Результати тестування показали, що запропонована система має більшу швидкодію (до 10 %) на відміну від аналогічних систем стиснення та шифрування інформації на основі дискретних відображень [15, 16]. Це зумовлене тим, що в системі, на відміну від аналогів, використовується простий метод шифрування та один генератор ПВП.

Висновки

Проведене дослідження генераторів псевдовипадкових послідовностей на основі дискретних відображень. Тестування статистичних властивостей проводилось з використанням пакету тестів NIST STS 2.1.2. Запропонований генератор псевдовипадкових послідовностей на основі комбінації лінійного конгруентного генератора та генератора на основі логістичного відображення для якого встановлено діапазон значень параметру керування λ при якому послідовності, генеровані запропонованим генератором задовольняють вимогам статистичних тестів. Проведені дослідження чутливості та криптостійкості генераторів псевдовипадкових послідовностей на основі дискретних відображень. Із результатів досліджень випливає наступне:

1. Поєднання генераторів псевдовипадкових послідовностей (лінійного конгруентного генератора та генератора на основі логістичного відображення), дозволяє збільшити діапазон значень параметру керування з $\lambda \in [3{,}99;4]$ (для генератора на основі логістичного відображення) до $\lambda \in [3{,}975;4]$ при якому послідовності, сформовані запропонованим генератором задовольняють вимогам статистичних тестів, що також підвищує криптостійкість генератора.

2. Проведені дослідження чутливості генератора ПВП на основі логістичного відображення до зміни параметру керування показали, що розбіжності в значеннях функції логістичного відображення з'являються вже при зміні параметра керування в десятому знаку при порозі розбіжності 0,00000001. Дослідження коефіцієнту кореляції між значеннями генерованих послідовностей показує, що найкращі властивості мають значення послідовностей починаючи з *N*-100 значень.

3. Проведений криптоаналіз генераторів на основі логістичного відображення з використанням атаки "груба сила", встановив, що для повного перебору ключів (при точності завдання параметрів керування в 11 знаків після коми) необхідно затратити 3,2 роки при значеннях параметра керування $\lambda \in [3{,}99;4]$ (для генератора на основі логістичного відображення), а при значеннях $\lambda \in [3{,}97;4]$ часові затрати становитимуть 9,5 років (для комбінації генераторів).

4. На основі розроблених генераторів ПВП та методів кодування інформації запропонована система кодування (стиснення) інформації з її додатковим шифруванням елементами хаотичної послідовності, генерованої на основі дискретних відображень. Результати тестування показали, що запропонована система має більшу швидкодію (до 10%) на відміну від аналогічних систем.

Література

1. Долгов В.А. Криптографические методы защиты информации : курс лекций / В.А. Долгов, В.В. Анисимов. – Хабаровск : Издательство ДВГУПС, 2008. – 155 с.

2. Kocarev L. Pseudorandom bits generated by chaotic maps / Kocarev L., Jakimoski G // Circuits and Systems I: Fundamental Theory and Applications, IEEETransactions. – 50(1). – 2003. – P. 123–126.

3. Гресь О.В. Дослідження криптостійкості хаотичних послідовностей генерованих на основі дискретних відображень / О.В. Гресь, Р.Л. Політанський, С.М. Храпко // Інформаційна безпека в сучасному суспільстві : матеріали І Міжнародної науково-практичної конференції, 21-22 листопада 2014 р., Львів. – С. 20-21.

4. Kanso A. Logistic chaotic maps for binary numbers generations / A. Kanso, N. Smaoui // Chaos, Solitons & Fractals. – 2009 – Vol. 40(5) – P. 2557–2568.

5. Гресь О. В. Дослідження статистичних характеристик генераторів бінарних послідовностей на

основі хаотичних відображень / О. В. Гресь, Р. Л. Політанський, Л. Ф. Політанський // Захист інформації і безпека інформаційних систем : матеріали V Міжнародної науково-технічної конференції, 2-3 червня 2016р. : тези доп. – Львів, 2016. – С. 118–119.

6. Гресь О.В. Дослідження криптостійкості генераторів бінарних послідовностей на основі дискретних відображень / О. В. Гресь, Р. Л. Політанський // Фізико-технологічні проблеми передавання, обробки та зберігання інформації в інфокомунікаційних : матеріалиV Міжнародної науково-практичної конференції, 3-5 листопада 2016р. : тези доп. – Чернівці, 2016. – С. 123.

7. Гресь О.В. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей / О.В. Гресь, Р.Л. Політанський, П.М. Шпатар, В.Я. Ляшкевич // Восточно-европейский журнал передовых технологий. – 2012. – № 6/11(60). – С. 8–10.

8. Гресь О.В. Алгоритм шифрування інформації з використанням псевдовипадкових послідовностей / О.В. Гресь, Р.Л. Політанський, П.М. Шпатар, А.Д. Верига // Наукові записки українського науково-дослідного інституту зв'язку. – 2013. – № 1(25). – С. 88–93.

9. Гресь О.В. Аналіз алгоритмів шифрування інформації на основі дискретнх вдображень / О.В. Гресь, В.М. Косован, М.І Скрипський, Г.М. Розорінов, П.М. Шпатар // Сучасний захист інформації. – 2015. – № 3. – С. 42–48.

10. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків : «Форт», 2012. – 880 с.

11. Болтенков В.А. Анализ алгоритмов хаотического шифрования изображений / Болтенков В.А., Никольский Е.С. // Цифрові технології. – 2010. – № 7. – С. 61–66.

12. PareekN.K. Cryptography using multiple one-dimensional chaotic maps / N.K. Pareek, Vinod Patidar, K.K. Sud // Commun. Nonlinear Sci. Numer. Simul. – 10(7). – 2005. – P.715–723.

13. Патент 82390, Україна, МПК(2013.01) H03M 7/00, H03M 7/30 (2006.01), H03M 13/07 (2006.01). Система кодування/декодування інформації з шифруванням / Політанський Л.Ф., Політанський Р.Л., Гресь О.В. ; заявник і власник ЧНУ ім. Ю.Федьковича. – № 201205880 ; заявл.14.05.12 ; опубл. 10.01.13, Бюл. № 1.

14. Политанский Р. Л. Система передачи данных с шифрованием хаотическими последовательностями / Р. Л. Политанский, П. М. Шпатарь, А. В. Гресь, А. Д. Верига // Технология и конструирование в электронной аппаратуре. – 2014. – № 2-3. – С. 28–32.

15. Bose R. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system / R. Bose, S. Pathak // IEEE transactions on circuits and systems: regular papers. – april 2006. – Vol. 53, NO. 4. – p. 848–857.

16. Wang B. Encrypting the compressed image by chaotic map and arithmetic coding / B. Wang, X. Zheng, S. Zhou, C. Zhou, X. Wei, Q. Zhang, C. Che // Optik. – 2014 . – Vol. 125 – p. 6117–6122

References

1. Dolgov V.A. Kriptograficheskie metodyi zaschityi informatsii. Kurs lektsiy. / V.A.Dolgov, V.V. Anisimov. – Habarovsk.: Izdatelstvo DVGUPS, 2008. – 155 s

2. Kocarev L. Pseudorandom bits generated by chaotic maps /Kocarev L., Jakimoski G //. –Circuits and Systems I: Fundamental Theory and Applications, IEEETransactions – 50(1) – 2003 – Pp. 123-126.

3. Hres O.V. Doslidzhennia kryptostiikosti khaotychnykh poslidovnostei henerovanykh na osnovi dyskretnykh vidobrazhen/O.V. Hres, R.L. Politanskyi, S.M. Khrapko // Informatsiina bezpeka v suchasnomu suspilstvi Materialy I Mizhnarodnoi naukovo-praktychnoi konferentsii, 21-22 lystopada 2014 r., Lviv, Ukraina – S. 20-21.

4. Kanso A. Logistic chaotic maps for binary numbers generations. / A. Kanso, N. Smaoui // Chaos, Solitons & Fractals. – 2009 – Vol. 40(5) – pp. 2557-2568.

5. Hres O. V. Doslidzhennia statystychnykh kharakterystyk heneratoriv binarnykh poslidovnostei na osnovi khaotychnykh vidobrazhen /O. V. Hres, R. L. Politanskyi, L. F. Politanskyi // Zakhyst informatsii i bezpeka informatsiinykh system: Materialy V Mizhnarodnoi naukovo-tekhnichnoi konferentsii, 2-3 chervnia 2016r.: tezy dop. – Lviv, 2016. – S. 118-119.

6. Hres O.V. Doslidzhennia kryptostiikosti heneratoriv binarnykh poslidovnostei na osnovi dyskretnykh vidobrazhen / Hres O. V., Politanskyi R. L. // Fizyko-tekhnolohichni problemy peredavannia, obrobky ta zberihannia informatsii v infokomunikatsiinykh: MaterialyV Mizhnarodnoi naukovo-praktychnoi konferentsii, 3-5 lystopada 2016r.: tezy dop. – Chernivtsi, 2016. – S. 123.

7. Hres O.V. Shyfruvannia informatsii z vykorystanniam psevdovypadkovykh hausovykh poslidovnostei / Politanskyi R.L., Shpatar P.M., Hres O.V., Liashkevych V.Ia. // «Vostochno-evropeiskyi zhurnal peredovykh tekhnolohyi». 2012 №6/11(60) S8-10.

8. Hres O.V. Alhorytm shyfruvannia informatsii z vykorystanniam psevdovypadkovykh poslidovnostei / Hres O.V., Politanskyi R.L., Shpatar P.M., Veryha A.D. // Naukovo-vyrobnychyi zbirnyk «Naukovi zapysky ukrainskoho naukovo-doslidnoho instytutu zviazku». 2013 №1(25) S88-93.

9. Hres O.V. Analiz alhorytmiv shyfruvannia informatsii na osnovi dyskretnkh vdobrazhen / O.V. Hres, V.M. Kosovan, M.I Skrypskyi, H.M. Rozorinov, P.M. Shpatar/ Suchasnyi zakhyst informatsii, №3, 2015, s. 42-48

10. Horbenko I.D. Prykladna kryptolohiia: Teoriia. Praktyka. Zastosuvannia: monohrafiia / I.D. Horbenko, Yu.I. Horbenko. – Kharkiv: «Fort», 2012. – 880 s.

11. Boltenkov V.A. Analiz algoritmov haoticheskogo shifrovaniya izobrazheniy / Boltenkov V.A., Nikolskiy E.S. // TsifrovI tehnologIYi/ # 7 – 2010 – S. 61-66.

12. PareekN.K. Cryptography using multiple one-dimensional chaotic maps / N.K. Pareek, Vinod Patidar, K.K. Sud // Commun. Nonlinear Sci. Numer. Simul – 10(7) – 2005 – Pp.715–723.

13. Politanskyi L.F., Politanskyi R.L., Hres O.V. Systema koduvannia/dekoduvannia informatsii z shyfruvanniam. Patent 82390, Ukraina, MPK(2013.01) H03M 7/00, H03M 7/30 (2006.01), H03M 13/07 (2006.01). zaiavnyk i vlasnyk ChNU im. Yu.Fedkovycha - №201205880; zaiavl.14.05.12; opubl. 10.01.13, Biul. №1

14. Politanskiy R. L. Sistema peredachi dannyih s shifrovaniem haoticheskimi posledovatelnostyami / Politanskiy R. L., Shpatar P. M., Gres A. V., Veriga A. D. // Tehnologiya i konstruirovanie v elektronnoy apparature. – 2014. – #2-3. – S. 28-32.

15. Bose R. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system / R. Bose, S. Pathak // IEEE transactions on circuits and systems—i: regular papers, . – april 2006 – Vol. 53, NO. 4 . – pp. 848-857

16. Wang B. Encrypting the compressed image by chaotic map and arithmetic coding / B. Wang, X. Zheng, S. Zhou, C. Zhou, X. Wei, Q. Zhang, C. Che // Optik. – 2014 . – Vol. 125 – pp. 6117–6122

Рецензія/Peer review : 27.06.2017 р. Надрукована/Printed :01.09.2017 р.
Рецензент: д.т.н., доц. Любчик В.Р.