В роботі запропонована програмна реалізація криптографічних алгоритмів, що базуються на властивостях хаотичних систем. Якісний аналіз отриманих результатів вказує на відсутність кореляції між даними і шифрованим текстом

Ключові слова: псевдовипадкова послідовність, шифрування, хаотична система

В работе предложена программная реализация криптографических алгоритмов, основанных на свойствах хаотических систем. Качественный анализ полученных результатов указывает на отсутствие корреляции между данными и зашифрованным текстом

Ключевые слова: псевдослучайная последовательность, шифрование, хаотическая система

The paper presents a software implementation of cryptographic algorithms, based on the properties of chaotic systems. Qualitative analysis of the results indicates to absence correlation between the data and the ciphertext

Keywords: pseudorandom sequence, encryption, chaotic system

УДК 621.391

МОДЕЛЮВАННЯ СХЕМ ШИФРУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Р.Л. Політанський
Кандидат фізико-математичних наук, доцент*
Контактний тел.: (037) 224-24-36
E-mail: polroos@mail.ru
Л.Ф. Політанський
Доктор технічних наук, професор, завідуючий кафедрою*
Контактний тел.: (037) 224-24-36
E-mail: rt-dpt@chnu.edu.ua
П.М. Шпатар
Кандидат технічних наук, доцент*
Контактний тел.: 050-978-50-14
E-mail: shpatar@ukr.net
О.В. Гресь
Аспірант*
Контактний тел.: 095-383-10-00
E-mail: alexgs85@ukr.net
*Кафедра радіотехніки та інформаційної безпеки
Чернівецький національний університет ім. Юрія Федьковича
вул. Коцюбинського, 2, м. Чернівці, 58012

Швидкий розвиток електронних засобів телекомунікацій сприяв розробці принципово нових методів передавання, зокрема криптографічних методів, що ґрунтуються на теорії динамічних систем з притаманними їм властивостями хаосу.

В роботі запропонована програмна реалізація криптографічних алгоритмів, що базуються на властивостях хаотичних систем. Прикладом хаотичних систем є псевдовипадкові послідовності. З точки зору криптографії представляють інтерес такі властивості хаотичних систем, як взаємно однозначна відповідність між хаотичними сигналами та інформаційними повідомленнями, близькі значення ймовірностей бітів “0” або “1”, асимптотична незалежність бітів “0” або “1”, достатньо великий період циклічності систем, висока чутливість до початкових умов.

Одним із поширених алгоритмів, що базуються на властивостях хаотичних систем є формування послідовності бітів, значення яких визначається належністю певного числа до однієї з двох підмножин $\left[0;\frac{1}{2}\right]$, $\left(\frac{1}{2};\ 1\right]$, на які розділяється множина дійсних чисел [0;1]. Математична модель формування псевдовипадкових послідовностей, що називається картою хаосу, для даного випадку має наступний вигляд:

$$b_i = \begin{cases} 0, \text{ при } x_i \in X_0 \\ 1, \text{ при } x_i \in X_1 \end{cases} \quad (1)$$

Така схема може описуватися одним або декількома параметрами, що є ключами криптографічної системи. Якщо схема описується одним параметром, то вона називається одновимірною, а якщо декількома параметрами – багатовимірною системою.

В загальному випадку схема генерування псевдовипадкових чисел описується виразом [1]:

$$x_{n+1} = (a \cdot x_n + d) \bmod N, \quad (2)$$

де x_n, x_{n+1} – значення системи на n-ій та n+1-ій ітерації; N – натуральне число, x_0, $a, d \in \{0, 1, \ldots, N-1\}$ – параметри системи, а “mod” означає арифметичний оператор знаходження залишку від результату ділення цілих чисел. Такий генератор є лінійним та періодичним, максимальне значення на виході якого досягається за наступних умов: числа d і N є взаємно простими; якщо деяке просте число p є дільником N, тоді число $a-1$ повинно бути кратним числу p.

Для одновимірної моделі генерування псевдовипадкових чисел може здійснюватися за наступними алгоритмами:

$$x_{n+1} = \begin{cases} ax_n, \text{при } x_n < \frac{1}{2}, 0 \le a \le 2 \\ a(1-x_n), \text{при } x_n \ge \frac{1}{2} \end{cases}, \quad (3)$$

$$x_{n+1} = \lambda x_n (1-x_n), \text{ при } 0 < \lambda \le 4 , \quad (4)$$

$$x_{n+1} = \frac{a}{4}\sin \pi x, \text{ при } 0 \le a \le 4 . \quad (5)$$

Вказані алгоритми шифрування реалізовані із використанням нелінійного зсувового регістру зі зворотним зв'язком CNFSR [3] (chaotic non-linear feedback shift register), схема якого приведена на рис. 1:

Параметрична булева функція, що використовувалась нами при дослідженнях має наступний вигляд:

$$b = \begin{cases} 0, \text{якщо } x_0^k \le x_e^k \\ 1, \text{якщо } x_0^k > x_e^k \end{cases}, \quad (6)$$

де x_0^k та x_e^k – цілі числа, утворені непарними та парними бітами відповідно.

Розглядувана карта працює таким чином. Нехай на k-му кроці ітерації отримали ціле байтове число $x(k)$, яке можна представити у двійковому вигляді:

$$x(k) = x_7^k x_6^k x_5^k x_4^k x_3^k x_2^k x_1^k x_0^k$$

де x_i^k – це і-й біт цілого числа x(k).
Тоді

$$\left.\begin{aligned} x_e^k &= x_6^k x_4^k x_2^k x_0^k \\ x_0^k &= x_7^k x_5^k x_3^k x_1^k \end{aligned}\right\} \quad (7)$$

Знайдений біт b_i (6) записується як правий крайній біт нового байтового слова

$$x^*(k) = x_6^k x_5^k x_4^k x_3^k x_2^k x_1^k x_0^k \cdot b , \quad (8)$$

що використовується у наступній ітерації:

$$x(k+1) = (ax^*(k) + d) \bmod N . \quad (9)$$

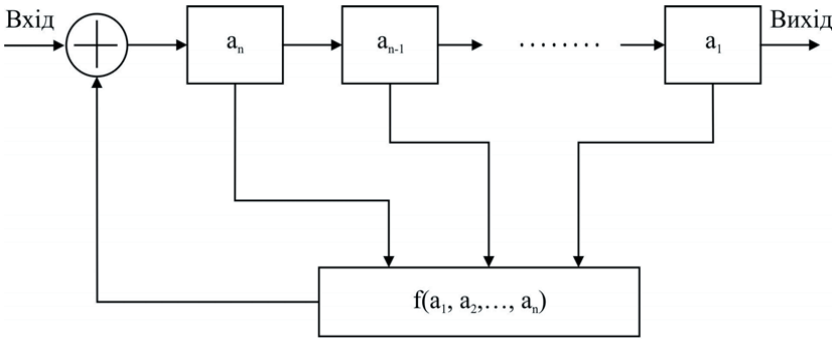


Рис. 1. Нелінійний регістр зі зворотнім зв'язком (CNFSR)

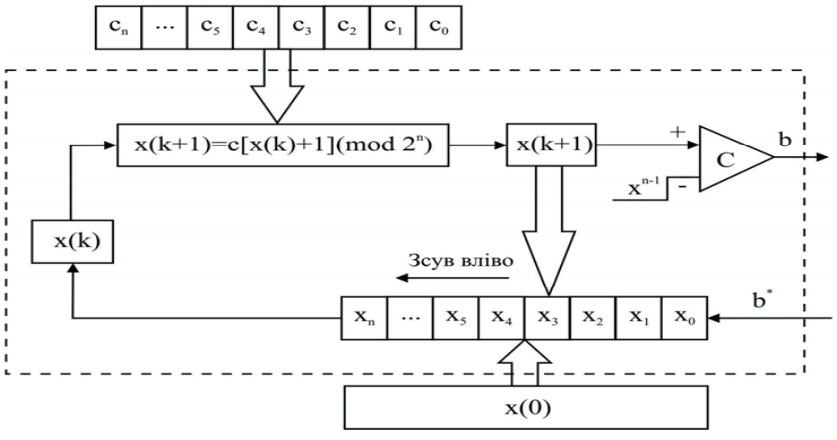


Рис. 2. Блок-схема алгоритму

Блок-схема вказаного алгоритму [2] приведена на рис. 2.

В даній роботі розглянута робота схеми за умови, що: d = c. Тобто двопараметрична схема була приведена до однопараметричної. Значення параметра c проходять всю множину байтових цілих чисел: c ∈ [1, 255].

Приведена схема була реалізована засобами програмування на мові C++.

Функції бібліотек наведені в табл. 1.

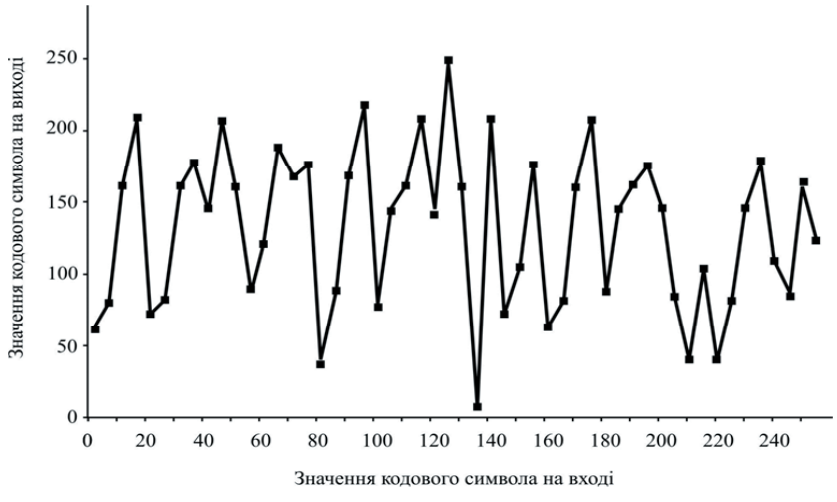
Таблиця 1

НАЗВА	ФУНКЦІЯ
Extern int byntodec(char*)	Перетворення послідовності нулів і одиниць, що утворюють значення текстового типу, у десяткове число
Extern char* dectobyn(int)	Перетворення десяткового числа у послідовність нулів і одиниць, що утворюють значення текстового типу
Extern int evenpart(int)	Утворення цілого числа, складеного із парних бітів цілого числа
Extern int oddpart(int)	Утворення цілого числа, складеного із непарних бітів цілого числа
Extern int step2(int)	Утворення цілого числа шляхом приєднання до нього біта і зсува вліво
Extern int step1(int,int)	Обчислення за формулою $x_{n+1} = (c \cdot (x_n + 1)) \bmod 2^n$ (c – параметр задачі)
Extern int output(int,FILE*)	Виведення кінцевих результатів у текстовий файл

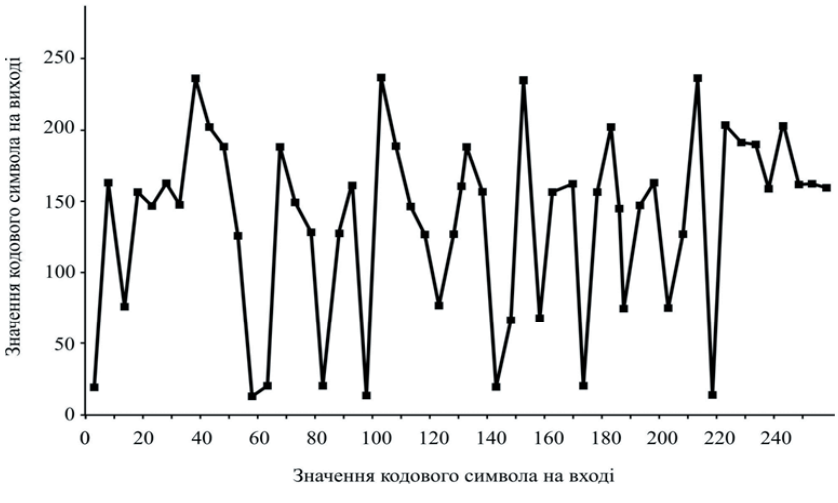
Засобами макрокоманд дані із текстових результатів переносяться у табличний процесор Microsoft Excel.

На рис. 3 приведена інтерпретація результатів інформаційного повідомлення при значеннях параметра c=21 та c=41, рис. 3, а і б відповідно.

Якісний аналіз отриманих результатів вказує на відсутність кореляції між даними і шифрованим текстом. Кількісне дослідження кореляції для вказаної схеми є результатом подальших досліджень.



а)



б)

Рис. 3. Результати шифрування байтових слів для двох значень параметра a, що дорівнюють 21 та 41 відповідно

Висновки

1. Дослідження складних криптосистем, які в подальшому реалізують у вигляді апаратних блоків можливо здійснити програмними засобами.

2. Властивості описаного алгоритму суттєво залежать від параметрів схеми.

3. Можливість описати криптосистеми функціональною залежністю є ускладненою внаслідок слабкої кореляції між початковим текстом і шифротекстом.

Література

1. Chen G. A symmetric image encryption scheme based on 3D chaotic cat maps/ Guangrong Chen, Yaobin Mao, Charles K. Chui // Chaos, Solutions and Fractals) - 2004 - 21. pp. 749-761.

2. Mao Y. A Chip Performing Chaotic Stream Encryption / Yaobin Mao, Wenbo Liu, Zhong Li, Ping Li, Wolfgang A. Halang // Studies in Computational Intelligence (SCI) - 2007 - 42. pp. 307-332.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение./ Б. Скляр. – М.: Издательский дом «Вильямс», 2007. – 1104с.