

Література

1. Артамонов Є.Б. Підхід до моделювання систем теплопостачання через аналіз причин виникнення втрат теплової енергії і теплоносія в системі / Є.Б. Артамонов // Математичні машини і системи. – 2007. – № 3,4. – С. 203-210.
2. Евдокимов А.Г. Информационно-аналитические системы управления инженерными сетями жизнеобеспечения населения / А.Г. Евдокимов, В.А. Петросов : Харьков: ХТУРЭ, 1998. – 412 с.
3. Соколов Е.Я. Теплофикация и тепловые сети: учебник для вузов / Е.А. Соколов . – изд. 7-е, стереот. – М.: Издательство МЭИ, 2001. – 472 с.
4. Артамонов Є.Б. Метод визначення несправних ділянок інженерної мережі (на прикладі теплових мереж) / Є.Б. Артамонов // Проблеми інформатизації та управління. – К.: НАУ. – 2010. – Вип. 1(29). – С. 12-19.
5. Гафаров А.Х. Анализ эффективной и надежной работы системы теплоснабжения / А.Х. Гафаров // Новости теплоснабжения. – 2003. – №5. – С. 25-30.
6. Теплові мережі: навч. посібник / за ред. М. О. Прядка. – К.: Алерта, 2005. – 227 с.
7. Современные информационные технологии в эксплуатации инженерных сетей / С.Г. Слюсаренко, В.П. Рожков, С.А. Субботин. и др. // Труды Междунар. науч.-практич. конф. «Геоинформатика-2000», 15–18 сентября 2000, Томск. – С. 219–224.
8. Ротштейн А.П. Медицинская диагностика на нечеткой логике / А.П. Ротштейн. – Винница: Континент-ПРИМ, 1996. – 132 с.

УДК 621.391

Гресь О.В., асп.; **Політанський Р.Л.,** к.ф.-м.н.; **Шпатар П.М.,** к.т.н.; **Верига А.Д.,** к.т.н.
(Чернівецький національний університет імені Юрія Федьковича)

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Гресь О.В., Політанський Р.Л., Шпатар П.М., Верига А.Д. Алгоритм шифрування інформації з використанням псевдовипадкових послідовностей. В даній роботі запропонований модифікований алгоритм шифрування інформації, з використанням послідовностей псевдовипадкових дійсних чисел, розподілених за гаусовим законом. Дослідження алгоритму на криптостійкість підтверджують можливість використання такого алгоритму для шифрування інформації.

Ключові слова: ПСЕВДОВИПАДКОВА ПОСЛІДОВНІСТЬ, ГЕНЕРАТОР, РОЗПОДІЛ ГАУСА, КРИПТОСТІЙКІСТЬ

Гресь А.В., Политанский Р.Л., Шпатар П.М., Верига А.Д. Алгоритм шифрования информации с использованием псевдослучайных последовательностей. В данной работе предложен модифицированный алгоритм шифрования информации, с использованием последовательностей псевдослучайных действительных чисел, распределенных по Гауссовскому закону. Исследование алгоритма на криптостойкость подтверждают возможность использования такого алгоритма для шифрования информации.

Ключевые слова: ПСЕВДОСЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, ГЕНЕРАТОР, РАСПРЕДЕЛЕНИЕ ГАУССА, КРИПТОСТОЙКОСТЬ

Hres' O.V., Polityanskiy R.L., Shpatar P.M., Veryha A.D. Data encryption algorithm using pseudorandom sequences. In this paper proposed a modified algorithm for encrypting information using pseudorandom sequences of real numbers, distributed by the Gaussian law. Research on algorithm to cryptographic confirm the possibility of using this algorithm to encrypt the information.

Keywords: PSEUDO-RANDOM SEQUENCE, GENERATOR, GAUSS DISTRIBUTION, CRYPTOGRAPHIC

Перспективним напрямком розвитку засобів телекомунікацій є використання в системах передавання інформації нових методів кодування, шифрування та передавання інформації, зокрема криптографічних методів, що базуються на використанні динамічних систем.

У існуючих методах та алгоритмах шифрування, особливо поточкових шифрах, використовуються генератори псевдовипадкових послідовностей (ПВП), що видають потік бітів, який може бути відтвореним одержувачем інформації, а для стороннього спостерігача є випадковим. Чим більша подібність генерованого потоку випадковому, тим більше часу необхідно затратити криптоаналітику для розкриття шифру [1].

1. Алгоритм шифрування. В даній роботі запропонований модифікований алгоритм шифрування інформації, з використанням генераторів ПВП, з гаусовим розподілом [2].

В загальному випадку схема генерування ПВП чисел описується виразом [2]:

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

де x_n, x_{n+1} – значення системи на n -ій та $n+1$ -ій ітерації; $x_0, a, d \in \{0, 1, \dots, N-1\}$ – параметри системи; N – натуральне число, а «mod» означає арифметичний оператор знаходження залишку від результату ділення цілих чисел.

Алгоритм шифрування базується на використанні в якості ключа генератора ПВП. Схема генерування ключа використовує два незалежних генератори ПВП (лінійний конгрудентний генератор та генератор на основі логістичного відображення), що працюють з різними початковими умовами:

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

де a_1, d_1, λ, x_0 – початкові умови для генерування послідовностей.

Вихідні послідовності цих генераторів за допомогою алгоритму Бокса-Мюллера перетворюються в послідовність, розподілену за законом Гауса [3].

Блок-схема алгоритму шифрування приведена на рис. 1.



Рис. 1. Блок-схема алгоритму шифрування

Роботу алгоритму розглянемо на прикладі шифрування повідомлень. Алгоритм шифрування здійснюється наступним чином. Вихідне повідомлення перетворюється в 8-и бітові числа згідно ASCII коду, утворюючи множину M_n .

Послідовність дійсних чисел з перетворюється в двійкове 8-и бітове представлення за допомогою наступної формули:

$$z_n = 0, b_{n1}, b_{n2} \dots b_{nL} = 2^{-1} b_{n1} + 2^{-2} b_{n2} + \dots + 2^{-L} b_{nL}, \quad (3)$$

де L – розрядність двійкового представлення.

Кількість згенерованих ключів шифрування рівна кількості символів в повідомленні. Множина Z_n утворюється як послідовність біт $\{b_{n1}, b_{n2} \dots b_{nL}\}$. Елементи інформаційного повідомлення m_n сумуються з елементами псевдовипадкової послідовності z_n з використанням операції XOR:

$$s_n = m_n \oplus z_n \quad (4)$$

Дешифрування здійснюється аналогічно завдяки зворотності операції XOR [4]. Блок-схема алгоритму дешифрування приведена на рис. 2.

Даний алгоритм дозволяє шифрувати не тільки текстові повідомлення, а й зображення. Для збільшення ефекту впливу змін вихідних даних на зашифровані, використаємо механізм дифузії, запропонований в [5]. Для випадку шифрування повідомлень даний механізм зв'язує значення шифрованих байтів з наступними байтами шифротексту.

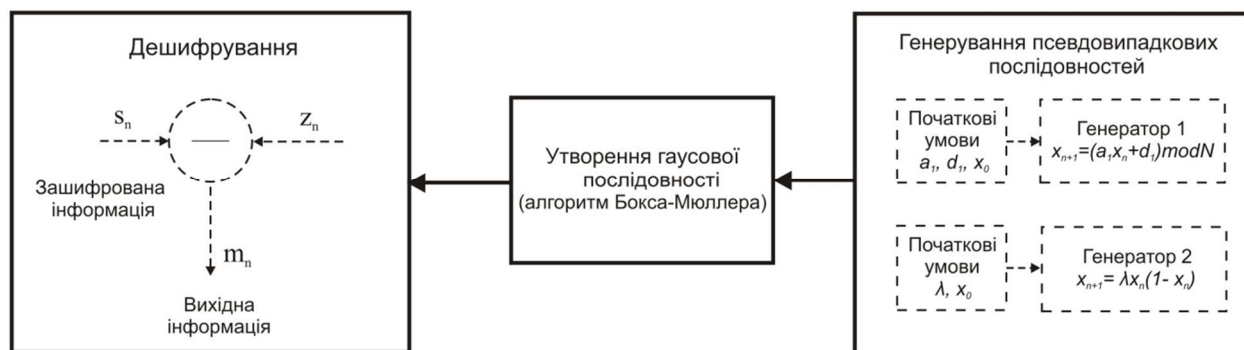


Рис. 2. Блок-схема алгоритму дешифрування

Механізм дифузії здійснюється за наступною формулою:

$$C(k) = \phi(k) \oplus \{I(k) + \phi(k)\} \bmod N \oplus C(k-1), \quad (5)$$

де $C(k-1)$ та $C(k)$ – попередній та наступний байти шифротексту, $I(k)$ – байт вихідного тексту, $\phi(k)$ – хаотична функція, в якості якої запропоновано логістичне відображення.

Обернене перетворення дифузії описується формулою:

$$I(k) = \{\phi(k) \oplus C(k) \oplus C(k-1) + N - \phi(k)\} \bmod N. \quad (6)$$

Параметрами перетворення дифузії є два початкові значення: $C(0)$ та $\phi(0)$. Ці параметри є додатковим ключем для алгоритму шифрування.

2. Реалізація алгоритму. Практична реалізація алгоритму здійснена в програмному середовищі Delphi 7.0. Часова діаграма ключової ПВП (після перетворення Бокса-Мюллера), що використовується для шифрування приведена на рис. 3.

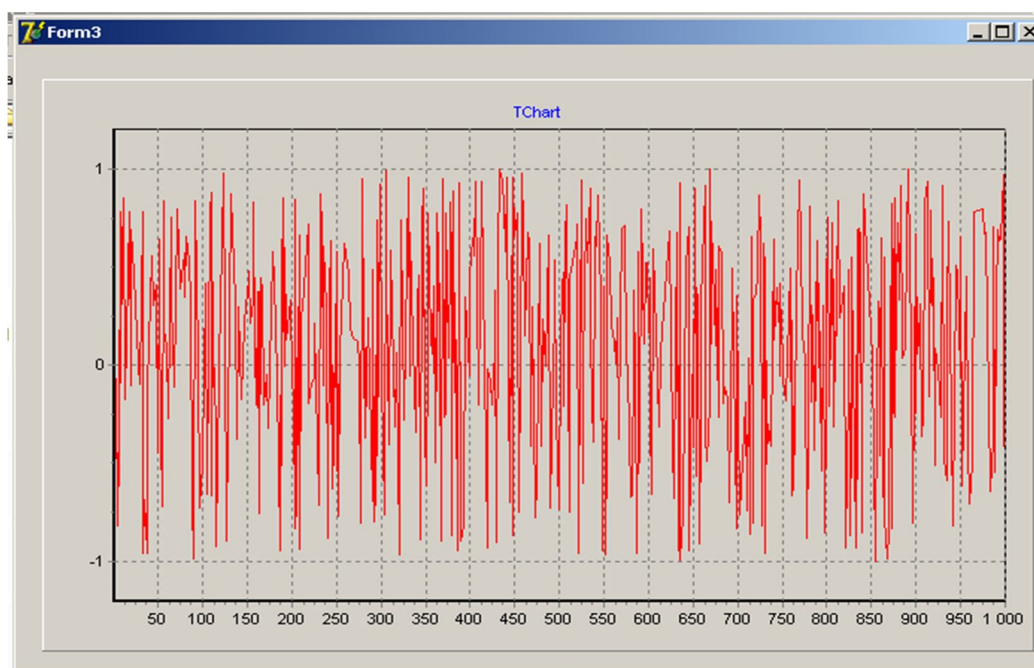


Рис.3. Псевдовипадкова ключова послідовність

Для демонстрації роботи алгоритму було взяте вихідне повідомлення “Чернівецький національний університет імені Юрія Федьковича”. На рис. 4 приведені вихідне та зашифроване повідомлення. Шифрування та дешифрування здійснюється за описаним алгоритмом. Оцінка ефективності алгоритму шифрування здійснювалась на прикладі шифрування зображень за значенням коефіцієнта кореляції між суміжними пікселями вихідного та зашифрованого зображень [6, 7].

Приклад шифрування зображень за допомогою даного алгоритму приведений на рис. 5.

Коефіцієнт кореляції між суміжними пікселями зображення визначається за наступною формулою:

$$C_p = \frac{N \sum_{j=1}^N x_j y_j - \sum_{j=1}^N x_j \sum_{j=1}^N y_j}{\sqrt{N \left\{ \sum_{j=1}^N x_j^2 - \left(\sum_{j=1}^N x_j \right)^2 \right\}} \sqrt{N \left\{ \sum_{j=1}^N y_j^2 - \left(\sum_{j=1}^N y_j \right)^2 \right\}}}, \quad (6)$$

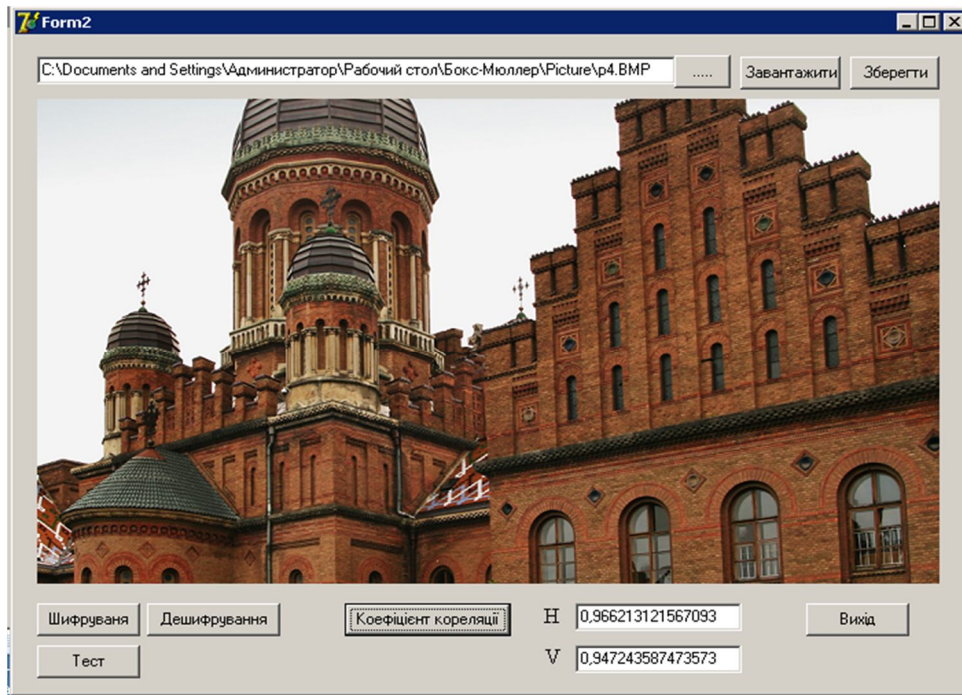
де x, y – значення градацій кольорів для двох суміжних пікселів зображення; N – число пікселів зображення які вибрані для розрахунку коефіцієнту кореляції.

Для вихідного зображення коефіцієнт кореляції становить 0,85...0,98.

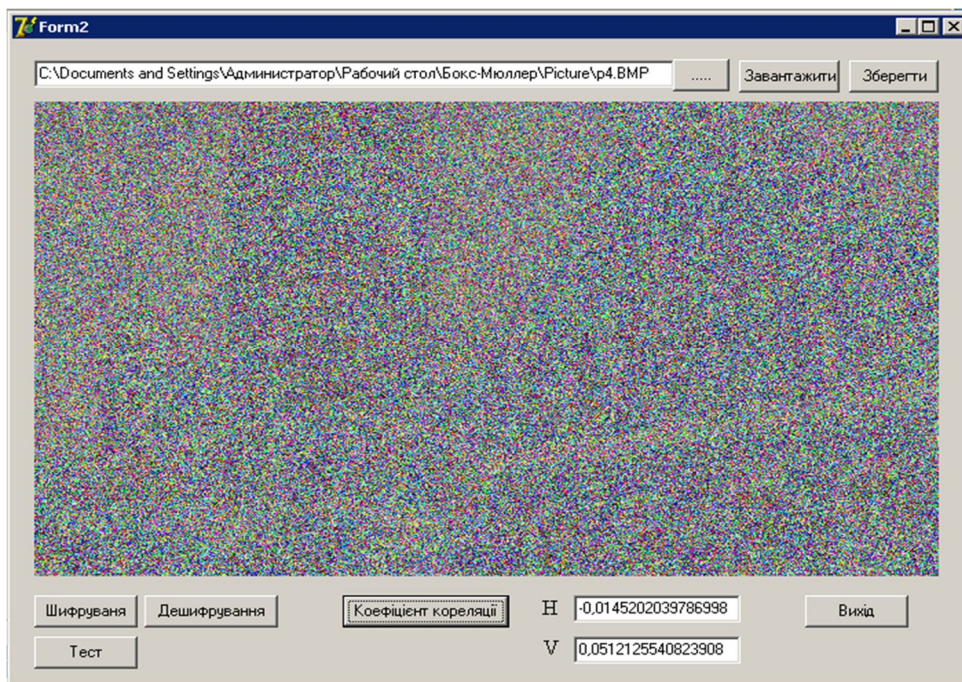
а)

б)

Рис. 4. Вихідне а) та зашифроване б) повідомлення



а)



б)

Рис.5. Вихідне а) та зашифроване б) зображення

Проведені експерименти з різними зображеннями показали, що коефіцієнт кореляції між суміжними пікселями зображень, зашифрованих запропонованим алгоритмом не перевищував 0,01...0,05. Отримані результати підтверджують криптостійкість шифрування зображень за запропонованим алгоритмом.

Висновки. В роботі продемонстровано модифікований алгоритм шифрування інформації, що базується на використанні в якості ключа двох генераторів ПВП, вихідні послідовності яких підпорядковуються розподілу Гауса. Дослідженнями показано, що в даному алгоритмі можливе поєднання лінійного та хаотичного (наприклад логістичне відображення) генераторів псевдовипадкових послідовностей, що підвищує криптостійкість системи. Крім шифрування текстових даних даний алгоритм також може шифрувати будь-

які інші файли, наприклад графічні. Отримані результати вказують на високу криптостійкість запропонованого алгоритму.

Література

1. Долгов В.А. Криптографические методы защиты информации. Курс лекций. / В.А. Долгов, В.В. Анисимов. – Хабаровск.: Издательство ДВГУПС, 2008. – 155 с.
1. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей / Р.Л. Політанський, П.М. Шпатар, О.В. Гресь, В.Я. Ляшкевич. // Восточно-европейский журнал передовых технологий. – 2012. – №6/11(60). – С8-10.
2. Преобразование Бокса-Мюллера [Электронный ресурс]. – Режим доступа : <http://ru.wikipedia.org>
3. Pareek N.K Image encryption using chaotic logistic map / Pareek N.K., Vinod Patidara, Sud K.K. // Image and Vision Computing 24. – 2006. – P. 926-934.
4. Chen Guanrong, Mao Yaobin, Chui Charles K. A Symmetric Image Encryption Scheme based on 3D Chaotic Cat maps // Chaos, Solitons and Fractals. – 2004. – V. 21, N 3. – P. 749-761.
5. Болтенков В.А. Анализ алгоритмов хаотического шифрования изображений / В.А. Болтенков, Е.С. Никольский // Цифрові технології. – 2010. – № 7. – С. 61-66.
6. Pareek N.K. Cryptography using multiple one-dimensional chaotic maps / Pareek N.K., Patidar V, Sud K. // Commun. Nonlinear Sci. Numer. Simul. – 2005. – №10(7). – P.715-723.
7. Liu S. An Improved Image Encryption Algorithm Based on Chaotic System / Liu S., Sun J., Xu Zh. // Journal of Computers. – 2009. – №11.Vol.4. – P. 1091-1100.

УДК 004.7

Кременецкий Г.М., к.т.н. (Національний авіаційний університет)

АНАЛИЗ ТА ФОРМУВАННЯ НЕОБХІДНИХ КОМАНД WEB-СЕРВІСІВ ДЛЯ СПЕЦІАЛІЗОВАНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ, ЩО ДИНАМІЧНО КЛАСТЕРИЗУЮТЬСЯ

Кременецкий Г.М. Анализ та формування необхідних команд WEB-сервісів для спеціалізованих обчислювальних мереж, що динамічно кластеризуються. Проведено порівняльний аналіз відомих реалізацій побудови WEB-сервісів стосовно побудови штучних нейронних мереж, що динамічно кластеризуються (REST та SOAP). Детально розглянуто життєві цикли розрахунків в обчислювальній мережі.

Ключові слова: НЕЙРОННА МЕРЕЖА, КЛАСТЕРИЗАЦІЯ, WEB-СЕРВІС, REST, SOAP.

Кременецкий Г.Н. Проведен сравнительный анализ известных реализаций построения WEB-сервисов относительно построения искусственных нейронных сетей, которые динамично кластеризируются (REST и SOAP). Детально рассмотрены жизненные циклы расчетов в вычислительной сети.

Ключевые слова: НЕЙРОННАЯ СЕТЬ, КЛАСТЕРИЗАЦИЯ, WEB-СЕРВИС, REST, SOAP

Kremenets'kyi H.M. Analysis and formation of necessary web-services commands to dynamical clustering specialized computer networks. A comparative analysis of known implementations of WEB-construction services relating to the construction of artificial neural networks, that clustering dynamically (REST and SOAP) was done. The life cycles of calculations in computer networks were regarded in details.

Keywords: NEURAL NETWORKS, CLUSTERING, WEB-SERVICE, REST, SOAP

1. Вступ. Сучасні розподілені додатки будуються на основі WEB-сервісів. Це дозволяє використовувати більшість існуючих можливостей Internet мережі та багато вже створених додатків на різних платформах і різних мовах програмування. Крім того, використання спеціальних UDDI (Universal Description Discovery and Integration) реєстрів WEB-сервісів дозволяє використовувати однакові сервіси, але від різних постачальників з різних серверів додатків. Тобто, існує безліч можливостей оптимізації розподілених обчислень як з точки зору фінансових витрат, так і швидкості обчислень.