УДК 004.056 (043.2)

Є. В. Ланських, *к.т.н., доцент*,
В. М. Зажома, *здобувач,*
С. В. Лада, *аспірант*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
e-mail: evlans@mail.ru

АЛГОРИТМ ГЕНЕРАЦІЇ ПЕРЕСТАНОВОК ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Стаття присвячена методу захисту інформації на основі матричних операцій криптографічного перетворення. Досліджено можливості застосування операцій перестановки для формування первинної матриці криптографічного перетворення, що є основою цього методу. Відповідно до отриманих результатів запропоновано нові перспективні способи та рекомендації щодо застосування операцій перестановки для матричного кодування. Проведено дослідження статистичних властивостей розроблених способів. За результатами тестування сформовано висновки щодо ефективності застосування запропонованих способів перестановки.

Ключові слова: *матричні операції, матричне кодування, криптографічне перетворення.*

Постановка проблеми. Сучасний розвиток інформаційного суспільства нерозривно пов'язаний з інтенсифікацією інформаційних процесів, необхідністю збору, обробки і передавання величезних обсягів інформації. Інформатизація торкнулася всіх сфер діяльності людини в цілому: державного управління, фінансів, економіки, освіти, виробництва та ін.

Неконтрольоване поширення і застосування інформаційних технологій призводить до втрати конфіденційності інформаційних ресурсів громадян і держави в цілому. Як наслідок, розвиток інформаційних ресурсів нерозривно пов'язаний з їх безпекою та захистом [1; 2].

Одним із найбільш дієвих засобів захисту інформаційно-телекомунікаційних систем є використання методів та засобів криптографії.

Основною задачею на сучасному етапі розвитку суспільства та його інформатизації є виконання вимоги постійного підвищення якості систем захисту інформації та оперативності обробки інформації і, перш за все, криптостійкості та оперативності функціонування систем криптографічного захисту інформації.

Аналіз останніх досліджень та публікацій. На сьогоднішній день одним із перспективних напрямів розвитку криптографії є використання розширеного спектра операцій криптографічного перетворення для вдосконалення існуючих та побудови нових криптоалгоритмів.

В роботах [3–5] запропоновано ряд нових операцій криптографічного перетворення на основі булевих функцій. Однак залишається невирішеним цілий ряд задач і проблем, зокрема побудова операцій криптографічного перетворення над великою кількістю змінних, розробка методів використання операцій криптографічного перетворення в алгоритмах та інші. Вирішення поставлених задач забезпечить підвищення якості та ефективності систем інформаційної безпеки.

Мета статті – провести дослідження нових способів генерації перестановок для покращення реалізації методу захисту інформаційних ресурсів на основі матричних операцій криптографічного кодування, що дозволить підвищити якість функціонування систем криптографічного захисту інформаційних ресурсів за рахунок підвищення швидкості реалізації шифрування та криптостійкості алгоритмів.

Виклад основного матеріалу дослідження. В роботах [6; 7] описаний новий перспективний метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення. Реалізація цього методу передбачає на початковому етапі на основі пароля формування первинної невиродженої матриці криптографічного перетворення. Для виконання вимог до існування операцій (матриць) перетворення, які забезпечують існування невиродженої матриці, синтез матриці проводиться на основі послідовного додавання за модулем два рядків матриці. Кількість доданків для син-

тезу кожного рядка мат-риці, а також номери доданків (рядків) визначаються паролем.

Оскільки формування первинної матриці криптографічного перетворення є основним і найважливішим етапом розробленого методу, то було проведено спробу розробити новий алгоритм формування первинної матриці шляхом використання операції перестановок.

У ході досліджень було запропоновано декілька способів виконання перестановок, а саме:

1. Для синтезу матриці криптографічного перетворення над кожним рядком початкової матриці відбувається одна операція перестановки. Тобто відбувається послідовна випадкова перестановка рядків матриці від першого до останнього.

2. Для синтезу матриці криптографічного перетворення над кожним рядком початкової матриці відбувається операція перестановки двічі. Тобто відбувається послідовна випадкова перестановка рядків матриці від першого до останнього, але, на відміну від першого варіанта, над кожним рядком матриці операція перестановки виконується двічі.

3. Для синтезу матриці криптографічного перетворення над кожним рядком початкової матриці відбувається операція перестановки тричі. Тобто відбувається послідовна випадкова перестановка рядків матриці від першого до останнього, але, на відміну від першого та другого варіантів, над кожним рядком матриці операція перестановки виконується тричі.

4. Для синтезу матриці криптографічного перетворення над кожним рядком початкової матриці відбувається операція перестановки, кількість повторень якої для кожного рядка визначається за допомогою функції random. Тобто відбувається послідовна випадкова перестановка рядків матриці від першого до останнього, але, на відміну від перших трьох варіантів, над кожним рядком матриці операція перестановки виконується деяку кількість разів залежно від випадкового значення.

5. Для синтезу матриці криптографічного перетворення застосовується спосіб № 1 з наступним додаванням постійного вектора інверсій (над результатами матричного перетворення відбувається криптографічне додавання з маскою інверсій).

6. Для синтезу матриці криптографічного перетворення застосовується спосіб № 2 з наступним додаванням постійного вектора інверсій.

7. Для синтезу матриці криптографічного перетворення застосовується спосіб № 3 з наступним додаванням постійного вектора інверсій.

8. Для синтезу матриці криптографічного перетворення застосовується спосіб № 4 з наступним додаванням постійного вектора інверсій.

9. Для синтезу матриці криптографічного перетворення над кожним рядком початкової матриці відбувається операція додавання за модулем 2, кількість та номери рядків, які додаються, визначаються за допомогою функції random. Синтез матриці відбувається доти, доки в кожному рядку не залишиться тільки по одній одиниці.

Для того щоб визначити ефективність застосування кожного з запропонованих способів формування первинної матриці криптографічного перетворення, проведено дослідження статистичних властивостей результатів криптографічного перетворення.

Для цього використано пакет NIST STS, який складається з 15 статистичних тестів, які використовуються для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини.

В основі статистичного тесту лежить перевірка деякої нульової гіпотези H_0 такої, що досліджувана послідовність – випадкова. Також передбачена альтернативна гіпотеза H_A, що припускає досліджувану послідовність невипадковою. Таким чином, після перевірки сгенерованої послідовності, для кожного тесту робиться висновок щодо відхилення, або прийняття нульової гіпотези H_0.

Для кожного тесту обирається адекватна статистика випадковості, на підставі якої далі відхиляється або приймається гіпотеза H_0. Така статистика, відповідно до припущення на випадковість, володіє деяким розподілом випадкових значень. Теоретично розподіл статистики для нульової гіпотези розраховується із застосуванням математичних методів. Далі із такого зразкового розподілу визначається критичне значення. Після проведення тесту розраховується значення тестової статистики, яке порівнюється із критичним значенням. При перевищенні тестового критичного значення над еталонним відхиляється нульова гіпотеза випадковості H_0. В іншому випадку робиться висновок про прийняття нульової гіпотези.

Із використанням 15 вбудованих тестів, що входять в пакет NIST STS, розраховується 189 ймовірностей P. Тому результатом тестування є побудова деякого вектора значень обрахованих імовірностей $P=\{P_1,P_2...,P_{189}\}$. Ці ймовірності можна розглядати, як окремі результати обчислень тестів.

Для здійснення тестувань було обрано такі параметри: довжина послідовності, що тестується, $n=10^6$ біт; кількість послідовностей, що тестується, $m=100$; рівень значущості; кількість тестів $q=189$.

Таким чином, обсяг вибірки, що тестується, становив $N=10^6\times100=10^8$ біт, кількість тестів (q) для різних довжин – $q=189$. Отже, статистичний портрет ПВП містить 18900 значень імовірності P.

В ідеальному випадку при $m=100$ і $\alpha=0{,}01$ у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має становити 99%. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу. Нижня межа дорівнює 0,96015.

Статистичні портрети відображають властивості випадковості результатів криптографічного перетворення на основі запропонованих способів.

Оскільки результати тестування перших чотирьох способів є незадовільними (не пройшли тест NIST STS), то немає сенсу відображати їх статистичні портрети. Статистичні портрети для інших способів зображено на рис. 1–5. Зведені результати тестування для запропонованих способів наведено в табл. 1.

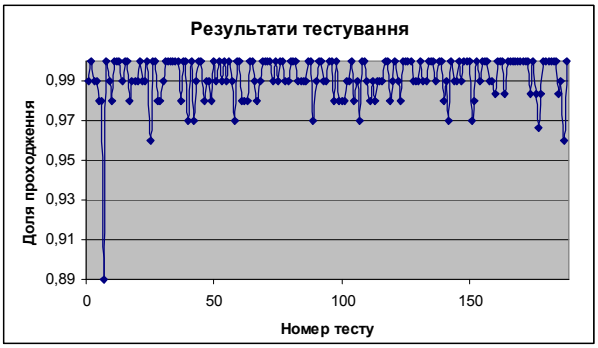

Рис. 1. Статистичний портрет результатів роботи 5-го способу синтезу матриці

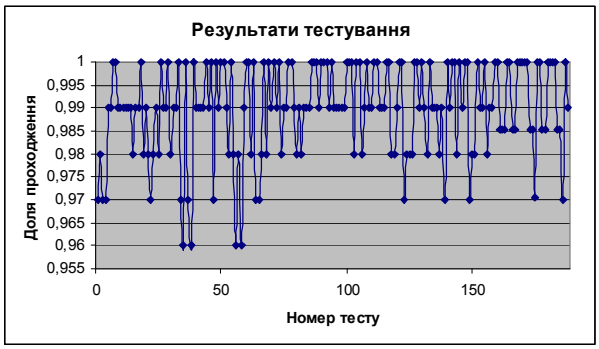

Рис. 2. Статистичний портрет результатів роботи 6-го способу синтезу матриці

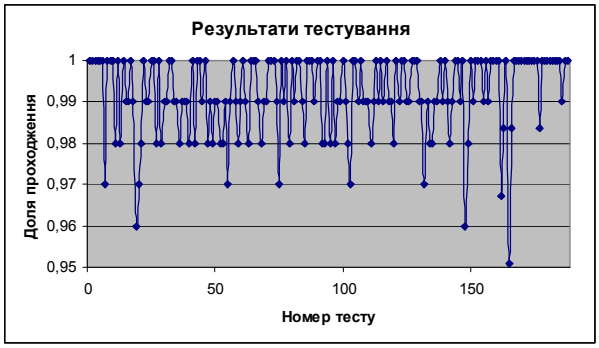

Рис. 3. Статистичний портрет результатів роботи 7-го способу синтезу матриці

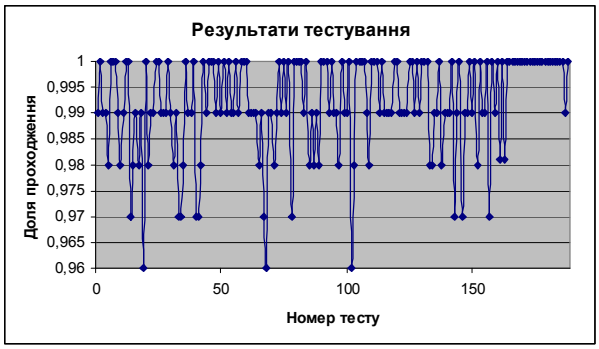

Рис. 4. Статистичний портрет результатів роботи 8-го способу синтезу матриці

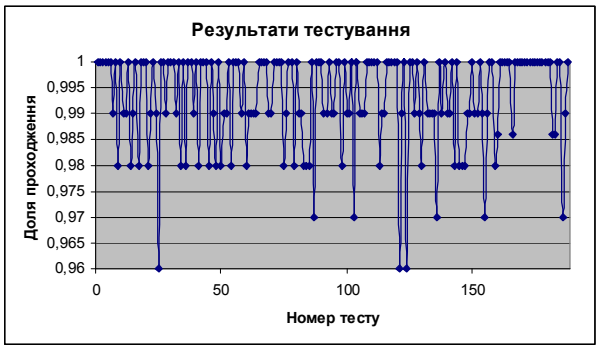

Рис. 5. Статистичний портрет результатів роботи 9-го способу синтезу матриці

Проаналізувавши дані з таблиці зведених результатів, можна зробити висновок, що найбільш ефективними є восьмий та девятий способи.

Таблиця 1

Зведені результати тестування

Способи реалізації	Кількість тестів, в яких тестування пройшло		Кількість тестів, в яких тестування не пройшло
	99% послід.	96% послід.	< 96% послід.
5-й спосіб	130 (68,8%)	188 (99,5%)	1 (0,5%)
6-й спосіб	147 (77,8%)	188 (99,5%)	1 (0,5%)
7-й спосіб	147(77,8 %)	188 (99,5%)	1 (0,5%)
8-й спосіб	153 (81,0%)	189 (100%)	0 (0%)
9-й спосіб	151 (79,9%)	189 (100%)	0 (0%)

Отримані результати показують, що запропоновані способи генерації перестановок можуть бути використані для формування первинної матриці криптографічного перетворення.

Висновки. Проведені обчислювальні експерименти дозволяють констатувати, що перетворення на основі перестановок покращує реалізацію методу захисту інформаційних ресурсів на основі матричних операцій криптографічного кодування. Запропонований алгоритм генерації перестановок дозволяє підвищити якість функціонування систем криптографічного захисту інформаційних ресурсів за рахунок підвищення швидкості реалізації шифрування та криптостійкості алгоритмів.

В результаті досліджень також було виявлено, що, якщо деяку послідовність випадкових чисел піддати матричному перетворенню за вищенаведеним алгоритмом, то якість випадкової послідовності покращується. Це, в свою чергу, може використовуватись для побудови якісних генераторів випадкових чисел.

Список літератури

1. Рябко Б. Я. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. – [2-е изд.]. – М. : Горячая линия-Телеком, 2013. – 232 с.
2. Юдин О. К. Захист інформації в мережах передачі даних / Юдин О. К., Корченко О. Г., Конахович Г. Ф. – К. : Вид-во ТОВ «НВП-ІНТЕРСЕРВІС», 2009. – 716 с.
3. Лужецький В. А. Використання операції множення за модулем в симетричних блокових шифрах / В. А. Лужецький, О. В. Дмитришин // Системи обробки інформації. – 2010. – № 5. – С. 9–14.
4. Дмитришин О. В. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 / О. В. Дмитришин. – Вінниця, 2012. – 180 с.
5. Рудницький В. М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В. М. Рудницький, В. Г. Бабенко, С. В. Рудницький // Захист інформації : наук.-практ. журн. –К. : НАУ, 2012. – № 3 (56). – С. 50–56.
6. Голуб С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – Вип. 3 (101), т. 1. – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 119–122.
7. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 163–168.

References

1. Ryabko, B. Ya. and Fionov, A. N. (2013) Foundations of modern cryptography and steganography. 2nd ed. Moscow: Goryachaya liniya-Telekom, 232 p. [in Russian].
2. Yudin, D. C., Korchenko, O. G. and Konahovich, G. F. (2009) Information security in data networks. Kyiv: Vyd-vo TOV «NVP-INTERSERVIS», 716 p. [in Ukrainian].
3. Luzhetskyy, V. A. and Dmytryshyn, O. V. (2010) The use of multiplication by module in

symmetric block ciphers. *Systemy obrobky informatsiyi*, (5), pp. 9–14 [in Ukrainian].
4. Dmytryshyn, O. V. (2012) Methods and means of block ciphering with high stability based on arithmetic operations by module. Ph.D. thesis. Vinnytsya, 180 p. [in Ukrainian].
5. Rudnytsky, V. M., Babenko, V. G. and Rudnytsky, S. V. (2012). The method of synthesis of matrix models for cryptographic operations of information recoding. *Zakhyst informatsiyi*: scientific-practical journal, 3 (56). Ktiv: NAU, pp. 50–56 [in Ukrainian].
6. Golub, S. V., Babenko, V. G. and Rudnytsky, S.V. (2012). The method of synthesis of cryptographic transformation operations based on addition by module two. *Systemy obrobky informatsiyi*: collection of scientific works, 3 (101), vol. 1. Kharkiv: KhUPS im. I. Kozheduba, pp. 119–122 [in Ukrainian].
7. Babenko, V. G. and Rudnytsky, S. V. (2012). Implementation of information security method based on matrix operations of cryptographic transformations. *Systemy obrobky informatsiyi* : of scientific works, 3 (101), vol. 1. Kharkiv: KhUPS im. I. Kozheduba, pp. 163–168 [in Ukrainian].

Стаття надійшла до редакції 23.09.2014.

Ye. V. Lanskykh, *Ph.D., associate professor,*
V. M. Zazhoma, *applicant for candidate,*
S. V. Lada, *post-graduate student*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
e-mail: evlans@mail.ru

THE ALGORITHM OF TRANSPOSITION GENERATION FOR INFORMATION SECURITY SYSTEMS

The article is devoted to information security method based on matrix operations of cryptographic transformation. The possibilities of using of transposition operations to form a primary cryptographic transformation matrix, which is the basis of this method, are investigated. According to obtained results new promising methods and recommendations on the use of transposition operations for matrix encoding are offered. The study of statistical properties of developed methods is carried out. According to test results the conclusions concerning the efficacy of proposed transposition methods are formed.

***Keywords**: matrix operations, matrix encoding, cryptographic transformation.*