ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 004.056.5 / С6

[0000-0003-2039-2841] **В. Г. Бабенко,** *д-р техн. наук, доцент,*
[0000-0002-7588-1055] **Т. В. Миронюк,** *канд. техн. наук, доцент,*
e-mail: t.myroniuk@chdtu.edu.ua
[0000-0002-5589-9020] **Г. В. Кривоус,** *аспірант*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

# АЛГОРИТМИ ЗАСТОСУВАННЯ ОПЕРАЦІЙ ПЕРЕСТАНОВОК, КЕРОВАНИХ ІНФОРМАЦІЄЮ, ДЛЯ РЕАЛІЗАЦІЇ КРИПТОПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

*У статті запропоновано застосування базової групи операцій перестановок, керованих інформацією, з урахуванням трьох видів алгоритмів реалізації криптографічного перетворення: просте перемішування, гамування з ключем, гамування з ключем із заданою кількістю раундів. Розроблено алгоритми використання операцій перестановок, керованих інформацією, з метою застосування їх як у програмних, так і в апаратних засобах криптографічного захисту інформації. Проведено оцінювання ефективності цих алгоритмів на основі їх програмної реалізації та статистичного тестування пакетом тестів NIST STS. Здійснено аналіз статистичних портретів одержаних результатів роботи розроблених алгоритмів з метою оцінки їх придатності в процесі побудови криптографічних алгоритмів. Показано, що для практичної реалізації криптографічного алгоритму на основі використання запропонованих операцій перестановок, керованих інформацією, потрібно визначити практичну криптографічну стійкість алгоритму, що напряму залежить від довжини пароля та кількості операцій, що застосовуються для шифрування інформації. Крім того, наведено розрахунок варіативності алгоритмів застосування для криптографічного перетворення декількох блоків інформації.*

***Ключові слова:*** *перестановка, базова операція, дискретна модель, криптографічне перетворення, статистичне тестування, раунд, псевдовипадкова послідовність, блок-схема алгоритму.*

**Вступ.** Застосування перестановки як однієї з базових операцій перетворення інформації характерне при вирішенні багатьох прикладних задач, наприклад, для захисту інформації при розробці алгоритмів блокового та потокового шифрування, для підвищення ефективності алгоритмів стиснення інформації при використанні перестановки в алгоритмах перетворення інформації з метою подання даних у зручнішому вигляді для подальшого стиснення, для реалізації алгоритмів кодування даних та багатьох інших [1-3]. Найпоширенішими базовими для симетричних криптографічних алгоритмів є такі типи перестановок: проста перестановка, одинарна перестановка з ключем, подвійна перестановка, перестановка «магічний квадрат», циклічна перестановка та комбінаційні перестановки [2, 5].

Для реалізації криптографічного перетворення інформації перестановки поєднують із додаванням за модулем, тому що ці операції доповнюють одна одну і в сукупності з іншими операціями забезпечують якість криптографічного перетворення. Виходячи з цього, було б доцільно поєднати в одній операції властивості як додавання за модулем, так і перестановок.

Розробка нових та вдосконалення поширених методів шифрування, які були б простими в апаратній та програмній реалізаціях і в той же час забезпечували досить високий рівень криптографічної стійкості за рахунок розширення спектра використовуваних операцій криптографічного перетворення, отриманих шляхом модифікації базових операцій, є одним із актуальних завдань інформаційної безпеки [1, 2].

Варто відзначити, що збільшення кількості операцій, придатних для реалізації криптографічних перетворень, має вагомі переваги: з одного боку, розширює можливості розробників криптографічних алгоритмів, а з другого – ускладнює роботу криптографічних аналітиків [1-3].


DOI: 10.24025/2306-4412.3.2021.247252

Пошук та синтез модифікованих операцій для криптографічного перетворення дадуть змогу будувати алгоритми з їх використанням із кращими криптографічними властивостями, що робить це дослідження актуальним.

Програмні засоби криптографічного захисту відрізняються гнучкістю, що дає їм особливу перевагу, порівняно з апаратними. А мобільність і простота використання пояснюють їх сучасну популярність та поширеність. Тому серед засобів поліпшення показників стійкості криптоалгоритмів можна виділити кілька підходів щодо побудови програмних шифрів. Найбільш перспективними для програмної реалізації є гнучкі шифри [5], що базуються на використанні декількох модифікацій алгоритму шифрування, шифри з псевдовипадковою вибіркою ключів і шифри з перестановкою фіксованих процедур та настроюванням операцій перетворення. Крім цього, одним із відомих способів підвищення криптостійкості є багатопрохідний режим застосування алгоритму шифрування [5, 6].

Застосування керованих операцій [5] відкриває великі можливості у досягненні необхідного рівня криптозахисту. Враховуючи те, що ефективність використання керованих операцій збільшується зі зростанням числа потенційно реалізованих модифікацій, оскільки в цьому випадку розширюється підблок даних, що перетворюються, набуває актуальності використання операції перестановки, бо вона має дуже велику кількість модифікацій [5]. Таким чином, розробка криптографічних засобів на основі керованих перестановок є перспективним напрямом у сучасній криптографії.

Особливу увагу в публікаціях з цієї тематики приділено математичним основам методів теорії захисту інформації, криптографії, цифрової стеганографії, а також особливостям їх реалізації та застосування [1-7].

Серед останніх досліджень і публікацій варто виділити дослідження [8, 9], де на основі синтезу та аналізу операцій двохоперандного додавання за модулем два та чотири здійснено моделювання двохоперандних дворозрядних матричних операцій, які мають властивості, необхідні для криптоперетворення, а в [10] проведено синтез та дослідження дворозрядного додавання за модулем два множини операцій криптографічного перетворення з точністю до перестановки, а також обґрунтовано можливість використання операцій виявленої групи як операції криптографічного додавання за модулем два. Роботи [11, 12] присвячені дослідженню груп операцій, синтезованих на основі додавання за модулем два, з точністю до перестановки з метою встановлення взаємозв'язків між групами та операндами. В [11] на основі визначених особливостей операцій групи виявлено взаємозв'язки між операціями, що дозволило використовувати синтезовані операції для прямого й оберненого перетворення інформації. В статті [12] представлено результати дослідження щодо застосування операцій додавання за модулем два та перестановки для розробки матричних операцій криптографічного перетворення. За результатами проведеного обчислювального експерименту здійснено поділ матричних моделей криптоперетворення на три групи за наявністю та типом перестановки в них.

У роботі [13] наведено результати дослідження статистичних властивостей сучасних потокових алгоритмів. Дослідження проводилися на основі методики статистичного тестування, що дозволило оцінити показники статистичної безпеки алгоритму, зокрема визначити непередбачуваність та випадковість формованих послідовностей, які є результатами роботи цих алгоритмів.

Проте дослідженню можливості використання групи операцій перестановок, керованих інформацією, для реалізації криптографічного перетворення не приділялось достатньої уваги.

**Мета та задачі дослідження:** розробка способів реалізації криптографічного перетворення інформації шляхом синтезу алгоритмів застосування операцій перестановок, керованих інформацією, та здійснення аналізу щодо їх придатності для використання в криптографічних алгоритмах.

**Виклад основного матеріалу.** Для розробки різних способів застосування операцій перестановок, керованих інформацією, при розробці алгоритмів реалізації криптографічного перетворення спочатку потрібно розглянути процес їх синтезу. При проведенні досліджень операцій криптографічного перетворення було встановлено, що загальна кількість цих операцій включає базові операції, операції перестановки та операції інверсії:


DOI: 10.24025/2306-4412.3.2021.247252

$$N = N_б \cdot N_n \cdot N_i = N_б \cdot 3! \cdot 2^3 = 384,$$

де $N$ – загальна кількість операцій, $N_б$ – кількість базових операцій, $N_n$ – кількість операцій перестановки, $N_i$ – кількість операцій інверсії [14, 15]. Отже, для визначення кількості, наприклад, трирозрядних базових операцій криптографічного перетворення необхідно вирахувати із загальної кількості операцій криптографічного перетворення кількість базових трирозрядних операцій.

У результаті розрахунків отримуємо, що кількість базових операцій для цього випадку $N_б = 8$.

У таблиці 1, де $F^k_{n,m,l}$ та $F^d_{n,m,l}$ – операції шифрування та розшифрування відповідно, а *n, m, l* – номери елементарних функцій перетворення, з яких утворена операція, представлено дискретну модель базових груп операцій, побудованих на основі визначених восьми базових операцій, що можуть бути використані для криптографічного перетворення інформації в системах захисту інформації [16].

Таблиця 1 – **Дискретна модель представлення криптографічних операцій шифрування-розшифрування**

| № | Базова група операцій шифрування | Базова група операцій розшифрування |
|---|---|---|
| 1 | $F^k_{92,46,27} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}$ | $F^d_{83,116,78} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}$ |
| 2 | $F^k_{53,71,27} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}$ | $F^d_{83,29,39} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ |
| 3 | $F^k_{83,29,39} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ | $F^d_{53,71,27} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}$ |
| 4 | $F^k_{58,29,78} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}$ | $F^d_{53,46,114} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ |
| 5 | $F^k_{58,116,39} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ | $F^d_{92,71,114} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ |
| 6 | $F^k_{53,46,114} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}$ | $F^d_{58,29,78} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}$ |


DOI: 10.24025/2306-4412.3.2021.247252

Закінчення таблиці 1

| № | Базова група операцій шифрування | Базова група операцій розшифрування |
|---|---|---|
| 7 | $F^{k}_{92,71,114} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3 \end{bmatrix}$ | $F^{d}_{58,116,39} = \begin{bmatrix} \overline{x}_1 \cdot x_2 \vee x_1 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \overline{x}_3 \end{bmatrix}$ |
| 8 | $F^{k}_{83,116,78} = \begin{bmatrix} x_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot x_3 \end{bmatrix}$ | $F^{d}_{92,46,27} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \vee x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}$ |

З метою перевірки коректності результатів, отриманих експериментальним способом для базових груп операцій шифрування-розшифрування, було розроблено програмне забезпечення на основі таких алгоритмів:

1. Простого перемішування.

2. Виконання гамування з ключем.

3. Виконання гамування з ключем із заданою кількістю раундів.

Потрібно зазначити, що під час програмної реалізації вказаних вище алгоритмів ключова інформація передається закритим каналом зв'язку.

Алгоритм реалізації програмного забезпечення для шифрування-розшифрування інформації на основі базових операцій перестановок, керованих інформацією, отриманих шляхом обчислювального експерименту, розроблено на основі методу простого перемішування та зображено у вигляді блок-схеми на рисунку 1.

Відповідно до побудованої блок-схеми реалізації алгоритму роботи програмного засобу етапи його виконання складаються з наступних кроків:

1. Відкриваємо вхідний файл будь-якого типу та зчитуємо його дані.

2. Зчитування даних, що знаходяться у відкритому файлі, відбувається послідовно по три байти інформації.

3. Випадковим чином (з використанням генератора псевдовипадкової послідовності) перемішуємо прочитані три байти інформації.

4. Обираємо функцію шифрування для вибраних байтів.

5. Шифруємо прочитані три байти інформації обраним методом шифрування.

6. Випадковим чином інвертуємо кожен із зашифрованих байтів.

7. Записуємо отримані три байти інформації у результуючий (зашифрований) файл.

8. Здійснюємо перевірку умови: якщо не досягнуто кінця файлу, переходимо до пункту 2, інакше – продовжуємо кроки виконання алгоритму.

9. Процес роботи програми завершено.

Алгоритм роботи програмного продукту для розшифрування результуючого файлу представлено на рисунку 2. Опис кроків його реалізації аналогічний алгоритму шифрування, наведеному вище.

Однак при застосуванні лише одного запропонованого алгоритму роботи програмного засобу для шифрування та розшифрування інформації визначеною групою базових операцій не можна стверджувати, що зазначена базова група є ефективною при її реалізації. Тому нами запропоновано розробити ще два алгоритми реалізації криптографічного перетворення інформації на основі застосування отриманої групи базових операцій з метою перевірки правильності одержаних результатів.

Надалі запропоноване програмне забезпечення для реалізації перевірки правильності застосування отриманої групи базових операцій криптографічного перетворення було реалізовано для алгоритму на основі виконання гамування з ключем.


DOI: 10.24025/2306-4412.3.2021.247252

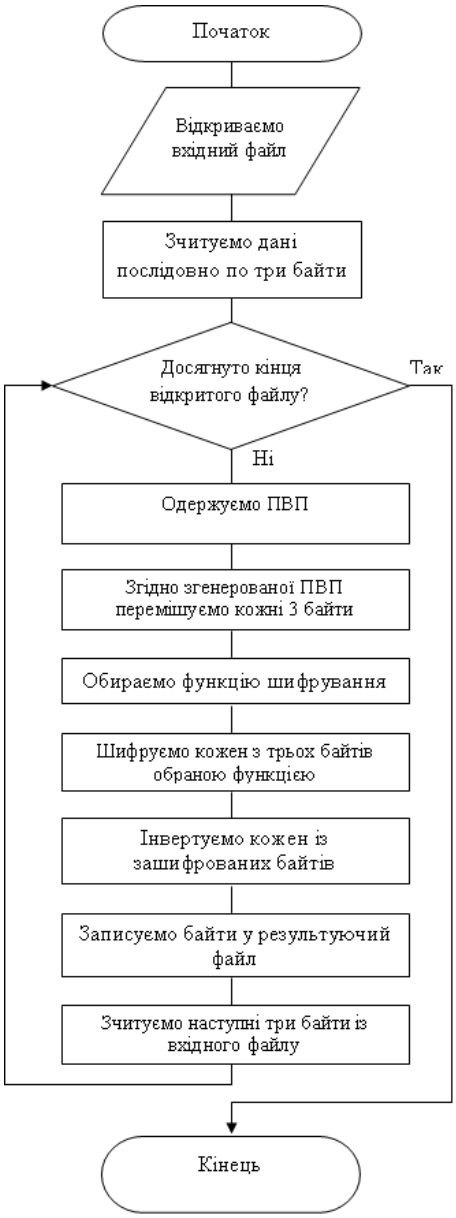


**Рисунок 1 – Граф-схема алгоритму шифрування вхідних даних визначеною групою базових операцій на основі простого перемішування**

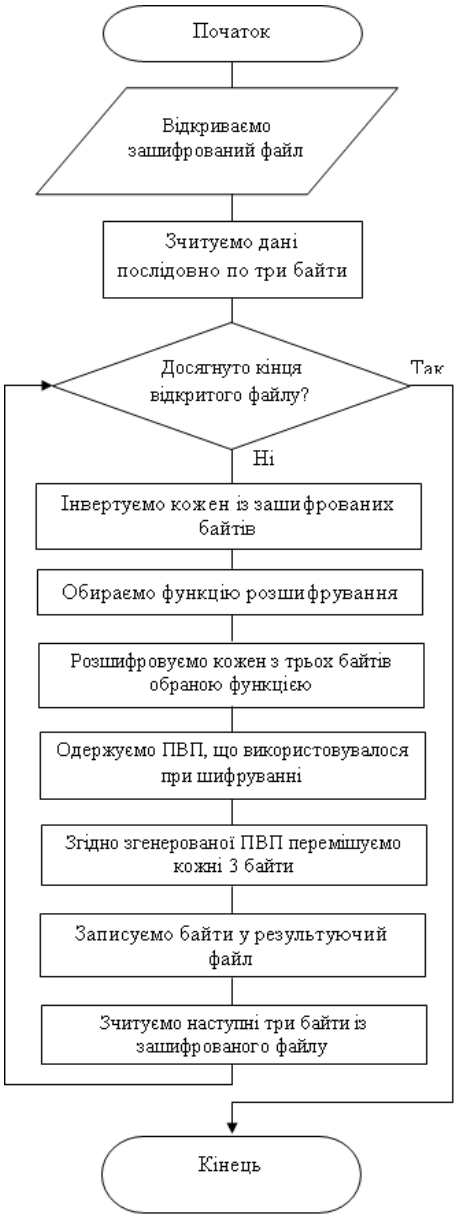


**Рисунок 2 – Граф-схема алгоритму розшифрування вхідних даних визначеною групою базових операцій на основі простого перемішування**

Алгоритм роботи запропонованого способу реалізації криптографічного перетворення складається з таких кроків:

1. Відкриваємо вхідний файл будь-якого типу та зчитуємо його дані.

2. Зчитуємо дані, що знаходяться у відкритому файлі, послідовно по три байти інформації.

3. Обираємо функцію шифрування для байтів інформації.

4. Шифруємо прочитані три байти інформації обраним методом шифрування.

5. Виконуємо процес гамування з ключем.

6. Отримані три байти інформації записуємо у результуючий файл.

7. У разі, якщо не було досягнуто кінця файлу, то переходимо до пункту 2.

8. Процес роботи програми завершено.

Алгоритм роботи відповідного методу розшифрування результуючого файлу описується аналогічно крокам, що реалізовують алгоритм шифрування.


DOI: 10.24025/2306-4412.3.2021.247252

Відповідно до алгоритму роботи описаного вище програмного засобу побудуємо блок-схеми способів реалізації методів шифрування та розшифрування інформації, які матимуть наступний вигляд та зображені на рисунках 3 та 4 відповідно.

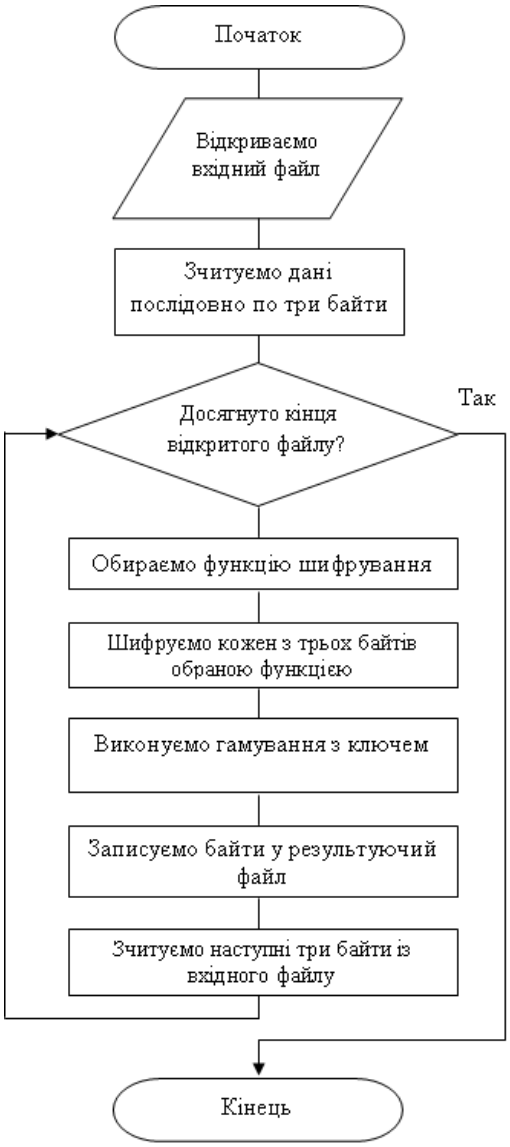


**Рисунок 3 – Граф-схема алгоритму шифрування вхідних даних визначеною базовою групою операцій на основі виконання гамування з ключем**

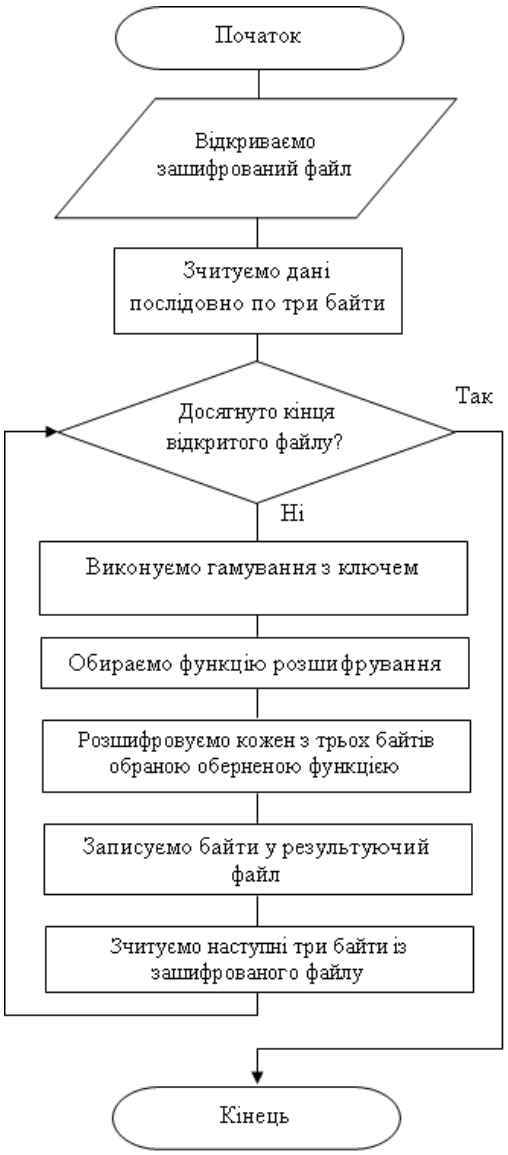


**Рисунок 4 – Граф-схема алгоритму розшифрування вхідних даних оберненою групою до визначеної базової групи операцій на основі виконання гамування з ключем**

Програмну реалізацію іншого способу криптографічного перетворення інформації, що забезпечується шифруванням даних визначеною базовою групою операцій, здійснено з використанням алгоритму на основі виконання гамування з ключем із визначеною кількістю циклів (раундів) перетворення даних та відображено у вигляді граф-схеми, наведеної на рисунку 5. На рисунку 6 наведено граф-схему реалізації алгоритму для розшифрування вхідних даних оберненою базовою групою операцій на основі виконання гамування з ключем із заданою кількістю циклів (раундів) перетворення інформації.


DOI: 10.24025/2306-4412.3.2021.247252

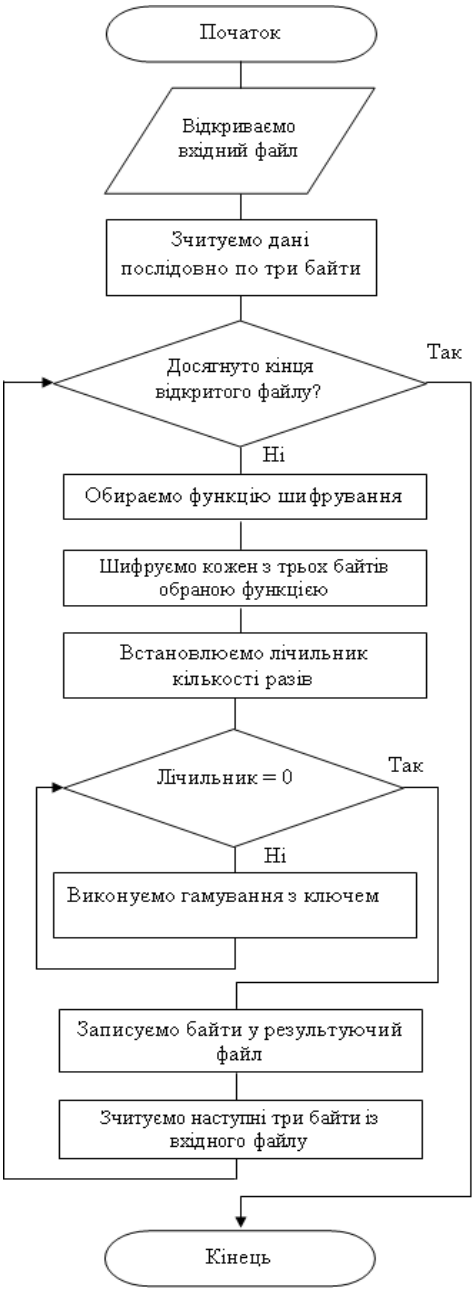


**Рисунок 5 – Граф-схема алгоритму шифрування вхідних даних базовою групою операцій на основі виконання гамування з ключем із заданою кількістю циклів (раундів) перетворення інформації**

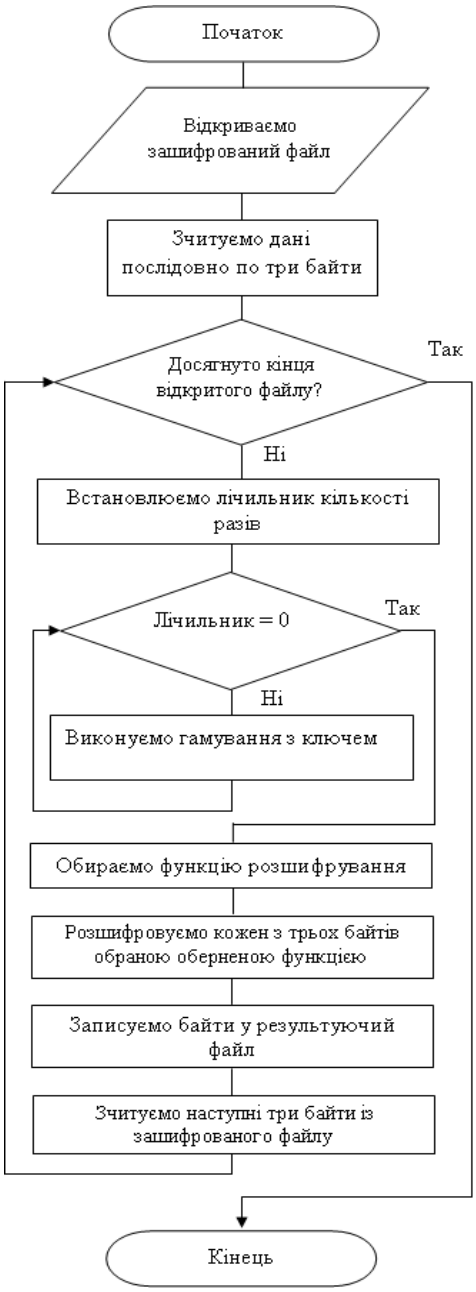


**Рисунок 6 – Граф-схема алгоритму розшифрування вхідних даних оберненою базовою групою операцій на основі виконання гамування з ключем із заданою кількістю циклів (раундів) перетворення інформації**

Алгоритм роботи реалізованого програмного продукту, що наведено на рисунку 5, складається з таких кроків:

1. Відкриваємо вхідний файл будь-якого типу та зчитуємо його дані.

2. Зчитуємо дані, що знаходяться у відкритому файлі, послідовно по три байти інформації.

3. Обираємо функцію шифрування для байтів інформації.

4. Шифруємо прочитані три байти інформації обраним методом шифрування.

5. Вказуємо кількість циклів (раундів) перетворення (шифрування).

6. Виконуємо гамування з ключем.

7. Здійснюємо перевірку умови: якщо лічильник раундів не рівний 0, виконуємо по-


DOI: 10.24025/2306-4412.3.2021.247252

вернення до пункту 6, інакше – продовжуємо виконання наступних кроків (до пункту 8).

8. Записуємо отримані три байти інформації у результуючий файл.

9. Здійснюємо перевірку умови: якщо не досягнуто кінця файлу, переходимо до пункту 2, інакше – пункт 10.

10. Завершення роботи програми.

Алгоритм роботи програмного забезпечення, розробленого для розшифрування результуючого (зашифрованого) файлу оберненою базовою групою операцій на основі виконання гамування з ключем заданою кількістю циклів (раундів), описується аналогічно до алгоритму шифрування.

**Результати дослідження.** Для перевірки ефективності розроблених алгоритмів роботи програмної реалізації способів шифрування та розшифрування інформації визначеною групою базових операцій перестановок, керованих інформацією, було проведено оцінювання статистичних властивостей результатів їх реалізацій за допомогою пакету статистичних тестів NIST STS [17]. NIST STS містить 15 статистичних тестів, що розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини [17, 20-22].

Для здійснення тестувань були обрані такі параметри: довжина послідовності, що тестується, $n = 10^6$ біт; кількість послідовностей, що тестується, $m = 100$; рівень значущості $\alpha = 0{,}01$; кількість тестів $q = 189$ [17-22].

Таким чином, обсяг вибірки, що тестується, становив $N = 10^6 \times 100 = 10^8$ біт, кількість тестів ($q$) для різних довжин $q = 189$. Отже, статистичний портрет ПВП містить 18 900 значень імовірності $P$ [17, 20].

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%. Однак це занадто жорстке правило, тому застосовується правило на основі довірчого інтервалу, згідно з яким нижня межа дорівнює 0,96015 [17, 20-22].

Результатом тестування алгоритму на основі простого перемішування з метою перевірки придатності використаних базових операцій для криптографічного перетворення є статичний портрет, що зображено на рисунку 7 [18].

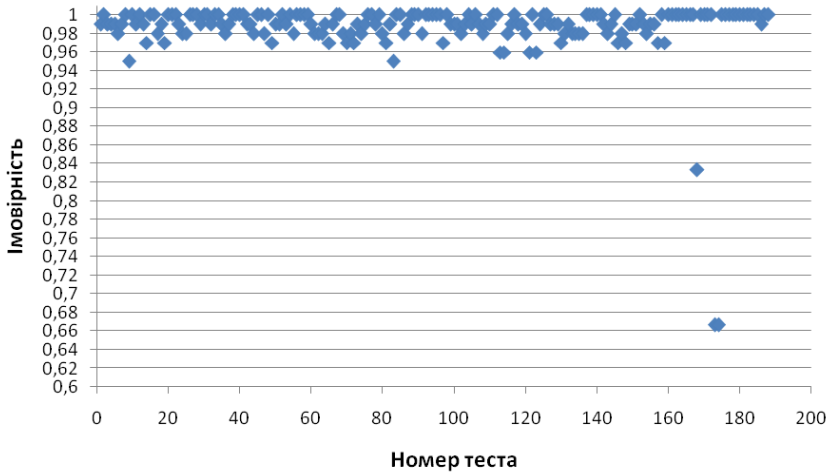


**Рисунок 7 – Графічна діаграма статистичних властивостей програмної розробки алгоритму на основі простого перемішування для криптоперетворення текстового файлу**

Підсумковий результат тестування визначеною базовою групою операцій за допомогою реалізованого алгоритму на основі простого перемішування програмним пакетом NIST STS наведено в таблиці 2.

Як видно з результатів (таблиця 3), п'ять тестів не було пройдено, а це означає, що досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS [17].

Результатом перевірки реалізованого алгоритму на основі гамування з ключем для криптоперетворення є графічна діаграма статичних властивостей, зображена на рисунку 8.


DOI: 10.24025/2306-4412.3.2021.247252

Таблиця 2 – **Зведені результати тестування текстового файлу базовою групою операцій перестановок, керованих інформацією, за допомогою алгоритму на основі простого перемішування**

| Генератор | Кількість тестів, які пройдено успішно, кількість (відсоток від загальної кількості) | |
|---|---|---|
| | 99 % послід. | 96 % послід. |
| Криптоалгоритм із застосуванням операцій перестановок, керованих інформацією | 137 (72,4 %) | 184 (97,3 %) |

Таблиця 3 – **Результати тестів, що не пройшли перевірку**

| РЕЗУЛЬТАТИ ДЛЯ РІВНОЙМОВІРНОСТІ Р-ЗНАЧЕНЬ І ПРОПОРЦІЇ (ЧАСТКА) ПОСЛІДОВНОСТЕЙ, ЩО ПРОЙШЛИ ТЕСТУВАННЯ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Р-ЗНАЧЕННЯ | ПРОПОРЦІЯ | НАЗВА СТАТИСТИЧНОГО ТЕСТУ |
| 11 | 13 | 10 | 9 | 11 | 13 | 7 | 12 | 3 | 11 | 0.494392 | 0.9500 * | Тест на збіг шаблонів, що не перекриваються |
| 12 | 12 | 10 | 9 | 11 | 15 | 5 | 12 | 3 | 11 | 0.249284 | 0.9500 * | |
| 2 | 1 | 2 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ---- | 0.8333 * | Варіант тесту на довільні відхилення |
| 2 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 2 | ---- | 0.6667 * | |
| 2 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | ---- | 0.6667 * | |

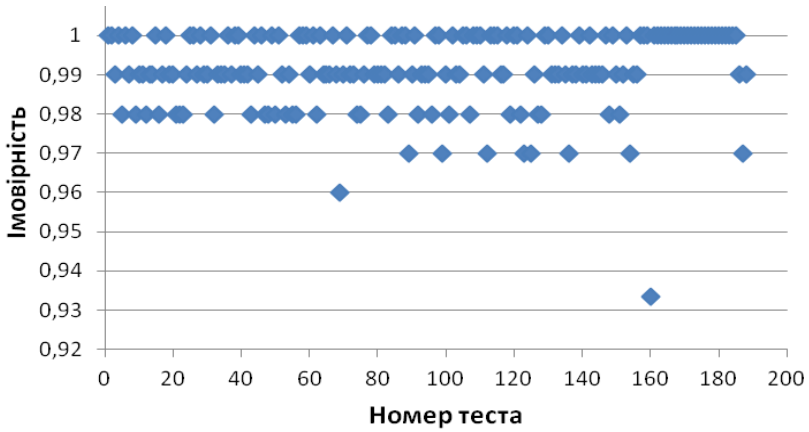


**Рисунок 8 – Графічна діаграма статистичних властивостей програмної розробки алгоритму на основі гамування з ключем для криптоперетворення текстового файлу**

Підведені результати тестування текстового файлу програмним пакетом NIST STS, що було сформовано із застосуванням алгоритму на основі гамування з ключем отриманою базовою групою операцій перестановок, керованих інформацією, подано в таблиці 4.

Як видно з результатів дослідження, послідовність не пройшла комплексний контроль за методикою NIST STS, оскільки не був пройдений один тест. Результати тестування наведено в таблиці 5.

Результатом перевірки програмної розробки алгоритму на основі гамування з ключем із заданою кількістю циклів (раундів) для криптоперетворення є графічна діаграма статистичних властивостей, наведена на рисунку 9.

Зведений результат тестування визначеної групи базових операцій перестановок, керованих інформацією, за допомогою розробленого алгоритму для криптографічного перетворення текстового файлу програмним пакетом NIST STS подано в таблиці 6.


DOI: 10.24025/2306-4412.3.2021.247252

Таблиця 4 – **Зведені результати тестування текстового файлу базовою групою операцій перестановок, керованих інформацією, за допомогою алгоритму на основі гамування з ключем**

| Генератор | Кількість тестів, які пройдено успішно, кількість (відсоток від загальної кількості) | |
|---|---|---|
| | 99 % послід. | 96 % послід. |
| Криптоалгоритм із застосуванням операцій перестановок, керованих інформацією | 148 (78,3 %) | 188 (95,5 %) |

Таблиця 5 – **Результати тестів, що не пройшли перевірку**

| РЕЗУЛЬТАТИ ДЛЯ РІВНОЙМОВІРНОСТІ P-ЗНАЧЕНЬ І ПРОПОРЦІЇ (ЧАСТКА) ПОСЛІДОВНОСТЕЙ, ЩО ПРОЙШЛИ ТЕСТУВАННЯ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | P-ЗНАЧЕННЯ | ПРОПОРЦІЯ | НАЗВА СТАТИСТИЧНОГО ТЕСТУ |
| 1 | 0 | 1 | 2 | 1 | 6 | 1 | 1 | 0 | 2 | 0.000648 | 0.9333 * | Тест на довільні відхилення |

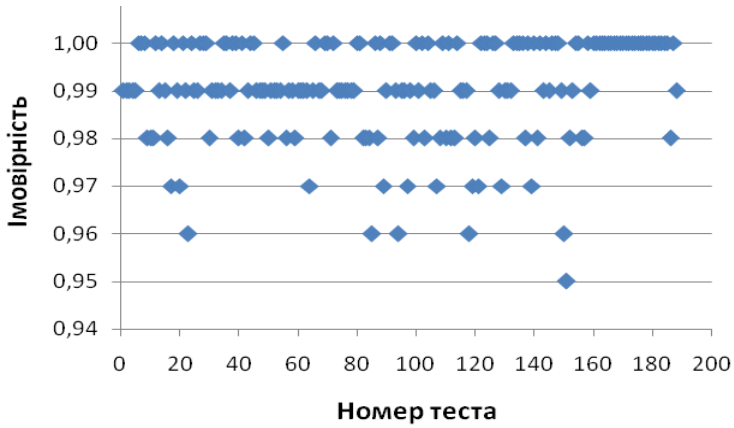


**Рисунок 9 – Графічна діаграма статистичних властивостей програмної розробки алгоритму на основі гамування з ключем із заданої кількості раундів для криптоперетворення текстового файлу**

Таблиця 6 – **Зведені результати тестування текстових даних з використанням базової групи операцій перестановок, керованих інформацією, за алгоритмом на основі гамування з ключем із заданої кількості циклів (раундів) перетворення інформації**

| Генератор | Кількість тестів, які пройдено успішно, кількість (відсоток від загальної кількості) | |
|---|---|---|
| | 99 % послід. | 96 % послід. |
| Криптоалгоритм із застосуванням операцій перестановок, керованих інформацією | 155 (81,4 %) | 188 (99,5 %) |

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS, тому що не був пройдений один тест (таблиця 7).


DOI: 10.24025/2306-4412.3.2021.247252

Таблиця 7 – **Результати тестів, що не пройшли перевірку**

| РЕЗУЛЬТАТИ ДЛЯ РІВНОЙМОВІРНОСТІ Р-ЗНАЧЕНЬ І ПРОПОРЦІЇ (ЧАСТКА) ПОСЛІДОВНОСТЕЙ, ЩО ПРОЙШЛИ ТЕСТУВАННЯ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Р-ЗНАЧЕННЯ | ПРОПОРЦІЯ | НАЗВА СТАТИСТИЧНОГО ТЕСТУ |
| 11 | 13 | 14 | 13 | 8 | 7 | 9 | 9 | 9 | 7 | 0.739918 | 0.9500 * | Тест на збіг шаблонів, що не перекриваються |

**Обговорення результатів.** Для розроблених алгоритмів роботи програмного засобу для шифрування та розшифрування даних певною групою базових операцій було проведено оцінку ефективності їх реалізацій за допомогою системи оцінки статистичних властивостей NIST STS [19, 20].

Отримані результати для алгоритмів, які реалізовані із застосуванням групи базових операцій перестановок, керованих інформацією, і використовуються з метою криптографічного перетворення текстової інформації, було перевірено за допомогою пакету тестів NIST STS [17, 21, 22]. Зведені результати тестування щодо використання операцій перестановок, керованих інформацією, для криптографічного перетворення представлено у таблиці 8.

Таблиця 8 – **Зведені результати тестування псевдовипадкових послідовностей, отриманих в процесі шифрування текстових даних, на основі алгоритмів із застосуванням операцій перестановок, керованих інформацією, для криптоперетворення**

| Алгоритм застосування операцій перестановок, керованих інформацією, для криптоперетворення | Кількість тестів з успішним тестуванням, кількість (відсоток від загальної кількості) | |
|---|---|---|
| | 99 % послід. | 96 % послід. |
| На основі простого перемішування | 137 (72,4 %) | 184 (97,3 %) |
| На основі гамування з ключем | 148 (78,3 %) | 188 (95,5 %) |
| На основі гамування із ключем із заданою кількістю циклів (раундів) перетворення інформації | 155 (81,4 %) | 188 (99,5 %) |

Аналіз результатів тестування пакетом тестів NIST STS запропонованих способів та алгоритмів реалізації операцій перестановок, керованих інформацією, з урахуванням псевдовипадкової (гамуючої) послідовності, показав, що статистичні властивості згенерованих послідовностей практично відповідають вимогам NIST STS, а наявні відхилення від вимог в межах від 0,5 % до 2,7 % обумовлені недостатньою кількістю операцій, що була відібрана для реалізації криптографічного перетворення під час проведення тестування. Тому доцільно використовувати їх з іншими алгоритмами криптографічного перетворення.

Щоб зашифрувати один блок інформації ($C$) використовується 384 отриманих операцій перестановок, керованих інформацією. Відповідно, для шифрування $m$ блоків інформації потрібно $C = m \cdot 384$ операції, що є варіативністю алгоритмів використання.

Наступним кроком буде визначення кількості алгоритмів обробки ($K_a$) інформації, що визначає довжину пароля, для визначених операцій перестановок, керованих інформацією, що дорівнює

$$K_a = \log_2 C . \qquad (1)$$

Виходячи з виразу (1), можна визначити, що кількість алгоритмів обробки для одного блоку інформації дорівнює $K_a = \log_2 384$.

Відповідно, кількість алгоритмів обробки для m блоків інформації буде дорівнювати $K_a = m \cdot \log_2 384 \approx 7 \cdot m$.


DOI: 10.24025/2306-4412.3.2021.247252

Визначимо практичну криптостійкість ( $R$ ), яка залежить від кількості операцій ( $K_o$ ), довжини пароля та криптографічного алгоритму, що було використано

$$R = K_a + K_o = m \cdot \log_2 384 + K_o \approx$$
$$\approx 7 \cdot m \cdot \log_2 K_o.$$

Дослідивши отримані результати, можна зробити висновок, що довжина пароля залежить від довжини інформації при застосуванні випадкового вибору операцій, керованих інформацією. Також можна зазначити, що довжина пароля при виборі операцій під час обробки кожного блоку дорівнює сім бітів.

При такому підході кількість байтів інформації, наприклад, для трирозрядних операцій, що реалізовують перестановки, керовані інформацією, можливо збільшити до $7 \cdot m$ разів.

**Висновки.** Наукова новизна цього дослідження полягає в тому, що вперше здійснено алгоритмізацію методу застосування групи операцій перестановок, керованих інформацією, для криптографічного перетворення інформації текстового файлу та проведено аналіз статистичних властивостей його результатів пакетом NIST STS.

У ході дослідження розроблених алгоритмів, що використовують операції перестановки, керовані інформацією, для криптоперетворення та аналізу їх результатів тестування, отриманих за допомогою пакета NIST STS, було визначено, що найефективнішим серед трьох алгоритмів є алгоритм на основі використання гамування з ключем із заданою кількістю раундів. Оскільки два інші алгоритми мають нижчу оцінку при статистичному тестуванні, застосовувати їх рекомендується разом з іншими алгоритмами криптографічного перетворення, щоб забезпечити необхідну криптографічну стійкість.

Практична реалізація криптографічного алгоритму та, відповідно, і алгоритми та способи застосування досліджуваних операцій перестановок, керованих інформацією, на основі яких будуються методи криптографічного перетворення інформації, напряму залежать від конкретних вимог, які сформульовані та визначені при синтезі систем захисту інформації.

Ефективність використання операцій перестановок, керованих інформацією, для криптографічного перетворення полягає у реалізації методу підвищення швидкості шифрування, сутність якого полягає у використанні послідовності, що гамує, як набору команд виконання послідовностей операцій криптографічного перетворення з використанням цих операцій перестановок. Якщо для шифрування одного блоку даних використовують 384 певні операції перестановок, керованих інформацією, то для *m* блоків інформації їх необхідно в *m* разів більше. Саме таким чином забезпечується варіативність алгоритмів, використаних під час криптографічного перетворення.

**Список використаних джерел**


[1] Ella Hassanien, and Mohamed Elhoseny, *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*. Springer Nature Switzerland AG, 2019.

[2] V. K. Pachghare, *Cryptography and Information Security*, third ed. PHI Learning Private Limited, 2019.

[3] Robert Ciesla, *Encryption for Organizations and Individuals*. Apress, Berkeley, CA. HELSINKI, Finland, 2020.

[4] D. J. Bernstein, "Fast-key-erasure random-number-generators", 2017. [Online]. Available: https://blog.cr.yp.to/ 20170723-random.html.

[5] А. А. Молдовян, Н. А. Молдовян, и Б. Я. Советов, *Криптография*. Санкт-Петербург, Россия: Лань, 2001.

[6] Б. Я. Рябко, и А. Н. Фионов, *Основы современной криптографии и стеганографии.* 2-е изд. Москва, Россия: Горячая линия - Телеком, 2013.

[7] Г. Ф. Конахович, и А. Ю. Пузыренко, *Компьютерная стеганография. Теория и практика*. Киев, Украина: МК-Пресс, 2006.

[8] В. Г. Бабенко, Н. В. Лада та С. В. Лада, "Синтез і аналіз мікроопераций для криптографічного перетворення", на *Другій міжнар. наук.-техн. конф. Проблеми інформатизації:* тези доп., Черкаси, 2014, с. 9-10.

[9] В. Г. Бабенко, та Н. В. Лада, "Синтез і аналіз операцій криптографічного додавання за модулем два", *Системи обробки інформації*, вип. 2 (118), с. 116-118, 2014.

[10] В. Г. Бабенко, та Н. В. Лада, "Дослідження множини операцій криптографічного



DOI: 10.24025/2306-4412.3.2021.247252

додавання", на *ІІ Міжнар. наук.-практ. конф. Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014)*: тези доп., Черкаси, 2014, т. 1, с. 135-136.

[11] В. Г. Бабенко, Н. В. Лада та С. В. Лада, "Аналіз множини операцій, синтезованих на основі додавання за модулем два" на *П'ятій міжнар. наук.-практ. конф. Методи та засоби кодування, захисту й ущільнення інформації*: тези доп., 2016, с. 54-57.

[12] В. Г. Бабенко, Н. В. Лада та С. В. Лада, "Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення", *Вісник Черкаського державного технологічного університету,* № 1, с. 5-11, 2016.

[13] О. О. Кузнецов, М. С. Луценко, А. В. Андрушкевич, О. М. Мелкозерова, Д. В. Новікова, та А. В. Лобан, "Статистичні дослідження сучасних потокових шифрів", *Прикладная радиоэлектроника*, № 3, т. 15, с. 167-178, 2016.

[14] В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко, Р. П. Мельник, С. В. Рудницкий, и О. Г. Мельник, *Криптографическое кодирование: методы и средства реализации*, часть 2. Харьков, Украина: Щедрая усадьба плюс, 2014.

[15] *Криптографічне кодування: обробка та захист інформації*, під. ред. В. М. Рудницького. Харків, Україна: ДІСА ПЛЮС, 2018.

[16] Т. В. Миронюк, "Визначення елементарних операцій базової групи перестановок, керованих інформацією", *Вісник Черкаського державного технологічного університету*, № 2, с. 100-105, 2016.

[17] J. Woodage, and D. Shumow, "An analysis of NIST SP 800-90A", in *Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science*, Y. Ishai and V. Rijmen, Eds., vol. 11477. Springer, Cham, 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-17656-3_6.

[18] Т. В. Миронюк, та В. Г. Бабенко, "Аналіз статистичних властивостей результатів криптографічного перетворення на основі операцій перестановок, керованих інформацією", на *Міжнар. наук.-практ. конф. Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук*: тези доп., 2017, т. 2, с. 41-47.

[19] Ю. В. Щербина, та С. Л. Волков, "Елементи практичної реалізації частотного тесту генераторів криптографічних перетворень", *Збірник наукових праць ОДАТРЯ*, вип. 2 (3), с. 17-21, 2013.

[20] А. В. Потій, С. Ю. Орлова, та Т. А. Гриненко, "Статистичне тестування генераторів випадкових і псевдовипадкових чисел з використанням набору статистичних тестів NIST STS". [Електронний ресурс]. Режим доступу: www.kiev-security.org.ua.

[21] A. Rukhin, J. Soto, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications". [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[22] В. В. Богданов, та Н. А. Паламарчук, "Навчальний комплекс статистичної оцінки псевдовипадкових і текстових послідовностей", *Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України "Київський політехнічний інститут"*, № 3, с. 17-26, 2007.

## References

[1] Ella Hassanien, and Mohamed Elhoseny, *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*. Springer Nature Switzerland AG, 2019.

[2] V. K. Pachghare, *Cryptography and Information Security*, third ed. PHI Learning Private Limited, 2019.

[3] Robert Ciesla, *Encryption for Organizations and Individuals*. Apress, Berkeley, CA. HELSINKI, Finland, 2020.

[4] D. J. Bernstein, "Fast-key-erasure random-number-generators", 2017. [Online]. Available: https://blog.cr.yp.to/ 20170723-random.html.

[5] A. A. Moldovian, N. A. Moldovian, and B. Ya. Sovetov, *Cryptography*. St. Petersburg, Russia: Lan, 2001 [in Russian].

[6] B. Ya. Ryabko, and A. N. Fionov, *Foundations of modern cryptography and steganography*, 2nd ed. Moscow, Russia: Goryachaya liniya - Telekom, 2013 [in Russian].

[7] G. F. Konahovich, and A. Yu. Puzyrenko, *Computer Steganography. Theory and Prac-*


DOI: 10.24025/2306-4412.3.2021.247252

*tice*. Kiev, Ukraine: MK-Press, 2006, [in Russian].

[8] V. H. Babenko, N. V. Lada, and S. V. Lada, "Synthesis and analysis of microoperations for cryptographic transformation", in *2nd Int. Sci.-Pract. Conf. Problems of informatization.* Cherkasy, 2014, pp. 9-10 [in Ukrainian].

[9] V. H. Babenko, and N. V. Lada, "Synthesis and analysis of cryptographic addition operations modulo two", *Systemy obrobky informatsii*, no. 2 (118), pp. 116-118, 2014 [in Ukrainian].

[10] V. H. Babenko, and N. V. Lada,, "Investigation of many cryptographic addition operations", in *2nd Int. Sci.-Pract. Conf. Information Technologies in Education, Science and Technology (ITONT-2014).* Cherkasy, 2014, vol. 1, pp. 135-136 [in Ukrainian].

[11] V. H. Babenko, N. V. Lada, and S. V. Lada, "Analysis of the set of operations synth-?sized on the basis of addition modulo two", in *5th Int. Sci.-Pract. Conf. Methods and means of coding, protection and consolidation of information,* Vinnytsia, 2016, pp. 54-57 [in Ukrainian].

[12] V. H. Babenko, N. V. Lada, and S. V. Lada, "Investigation of relationships between operations in matrix models of cryptographic transformation", *Visnyk Cherkaskogo derzhavnogo tekhnologich-nogo universytetu*, no. 1, pp. 5-11, 2016 [in Ukrainian].

[13] O. O. Kuznetsov, M. S. Lutsenko, A. V. Andrushkevych, O. M. Melkozerova, D. V. Novikova, and A. V. Loban, "Statistical studies of modern stream ciphers", *Prikladnaya radioelektronika*, no. 3, vol. 15, pp. 167-178, 2016 [in Ukrainian].

[14] V. N. Rudnitskiy, V. Ya. Milchevich, V. G. Babenko, R. P. Melnik, S. V. Rudnitskiy, and O. G. Melnik, *Cryptographic coding: methods and means of implementation*, part 2. Kharkov, Ukraine: Shchedraia usadba plius, 2014 [in Russian].

[15] *Cryptographic coding: information processing and protection*, V. N. Rudnytskyi, Ed. Kharkiv, Ukraine: DISA PLIUS, 2018 [in Ukrainian].

[16] T. V. Myroniuk, "Definition of elementary operations of the base group of permutations, controlled by information", *Visnyk Cherkaskogo derzhavnogo tekhnologich-nogo universytetu,* no. 2, pp. 100-105, 2016 [in Ukrainian].

[17] J. Woodage, and D. Shumow, "An analysis of NIST SP 800-90A", in *Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science*, Y. Ishai and V. Rijmen, Eds., vol. 11477. Springer, Cham, 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-17656-3_6.

[18] T. V. Myroniuk, and V. H. Babenko, "Analysis of statistical properties of cryptographic transformation results based on information-driven permutation operations", in *Int. Sci.-Pract. Conf. Innovative Current Trends in the Field of Natural Sciences, Humanities and Exact Sciences*, 2017, vol. 2, pp. 41-47 [in Ukrainian].

[19] Yu. V. Shcherbyna, and S. L. Volkov, "Elements of practical implementation of frequency test of generators of cryptographic transformations", *Zbirnyk naukovykh prats ODATRIA*, no. 2 (3), pp. 17-21, 2013 [in Ukrainian].

[20] A. V. Potii, S. Yu. Orlova, and T. A. Hrynenko, "Statistical testing of random and pseudo-random number generators using the NIST STS statistical test suite". [Online]. Available: www.kiev-security.org.ua.

[21] A. Rukhin, J. Soto, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications". [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[22] V. V. Bohdanov, and N. A. Palamarchuk, "Educational complex of statistical evaluation of pseudo-random and text sequences", *Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii Natsionalnoho tekhnichnoho universytetu Ukrainy "Kyivskyi politekhnichnyi instytut"*, no. 3, pp. 17-26, 2007 [in Ukrainian].


DOI: 10.24025/2306-4412.3.2021.247252

**V. H. Babenko,** *Dr. Tech. Sc., Associate Professor,*
**T. V. Myronyuk,** *Ph. D., Associate Professor,*
e-mail: t.myroniuk@chdtu.edu.ua
**H. V. Kryvous,** *Postgraduate*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

# ALGORITHMS FOR APPLICATION OF PERMUTATION OPERATIONS CONTROLLED BY INFORMATION FOR IMPLEMENTATION OF CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION

*The purpose and objectives of the study are to develop the ways to implement cryptographic transformation of information by synthesizing algorithms for permutation operations controlled by information, and to make the analysis of their suitability for use in cryptographic algorithms.*

*The article provides the use of the basic group of permutation operations controlled by information based on three types of algorithms for implementing the cryptographic transformation: simple shuffling, gamma sequence with a key, gamma sequence with a key with a given number of rounds. Algorithms for application of permutation operations controlled by information for the purpose of applying them in both software and hardware means of cryptographic information protection have been developed. The effectiveness of these algorithms has been evaluated on the basis of their software implementation and statistical testing by the NIST STS test package.*

*The analysis of statistical portraits of the received results of work of the developed algorithms for the purpose of an estimation of their suitability in the course of construction of cryptographic algorithms is carried out. It is shown that for practical implementation of cryptographic algorithm based on the use of proposed permutation operations controlled by information, it is necessary to determine the practical cryptographic stability of the algorithm, which directly depends on password length and number of operations used to encrypt information. In addition, the calculation of application algorithms variability for cryptographic transformation of several blocks of information is given.*

*The effectiveness of using permutation operations controlled by information for cryptographic transformation is to implement the method of increasing the encryption rate, the essence of which is to use a gamma sequence as a set of commands to execute sequences of cryptographic transformation operations using these permutation operations.*

*In the course of studying the developed algorithms for using permutation operations controlled by information for cryptographic transformation and analyzing their testing results obtained with the use of the NIST STS package, it has been determined that the most effective among the three algorithms is the algorithm based on the use of gamma with a key with a given number of rounds. Since the other two algorithms have a lower score in statistical testing, it is recommended to use them together with other cryptographic transformation algorithms in order to provide the necessary cryptographic strength.*

***Keywords:*** *permutation, basic operation, discrete model, cryptographic transformation, statistical testing, round, pseudo-random sequence, block diagram of the algorithm.*

*Стаття надійшла 24.09.2021*
*Прийнято 13.10.2021*


DOI: 10.24025/2306-4412.3.2021.247252