УДК 004.027

МЕТОД ФОРМУВАННЯ ПЕРЕСТАНОВОК ДОВІЛЬНОЇ КІЛЬКОСТІ ЕЛЕМЕНТІВ

Володимир Лужецький, Іван Горбенко

Базовими операціями будь-якого алгоритму шифрування є заміна та перестановка, тому для побудови криптографічно стійкого шифру потрібен надійний генератор перестановок. Сучасні шифри здійснюють перестановки лише в межах окремого блоку, а не блоків у межах всього повідомлення, що не дозволяє підвищити стійкість. Крім того, існуючі методи формування перестановок або взагалі не дають можливості сформувати окрему псевдовипадкову перестановку, або мають обмеження на кількість елементів опорної множини, або не забезпечують псевдовипадкового характеру перестановок та є складними з точки зору реалізації. Розроблено метод, який забезпечує формування псевдовипадкової перестановки довільної кількості елементів та є досить простим у реалізації за рахунок відсутності складних обчислень. Метод має вісім варіантів, які відрізняються статистичними характеристиками оцінки псевдовипадковості. Наведено алгоритм формування перестановок, математичну модель та оцінки порівняння розробленого методу з існуючими.

Ключові слова: *перестановка, псевдовипадкова перестановка, опорна множина, кількість елементів, складність реалізації, статистичні характеристики.*

Вступ. На даний час поширеними методами захисту інформації в комп'ютерних системах є криптографічні методи, серед яких важливе місце займають методи шифрування інформації.

Згідно К. Шеннона [1], будь-який алгоритм шифрування можна представити у вигляді комбінації операцій заміни та перестановки. Цей висновок реалізується в сучасних шифрах з використанням різних структурно-алгоритмічних підходів. Найпоширенішим є використання мереж Фейстеля з двома або чотирма гілками [2], SP-мереж [3], та матричних обчислень над двомірними представленнями даних [4]. Однак, варто відзначити, що ці підходи не повною мірою використовують можливість забезпечення стійкості шифру за рахунок виконання операції перестановки.

Усі відомі шифри будуються з використанням операції перестановки тільки в межах блоку. Наприклад, у блокових шифрах, побудованих на основі мереж Фейстеля, перестановка відбувається тільки для двох або чотирьох частин блоку, причому правило перестановки фіксоване і не залежить від секретного ключа. В блокових шифрах, побудованих на основі SP-мереж, перестановки відбуваються для кількості елементів більше чотирьох, але також в межах блоку, а не всього повідомлення. Це ж характерно і для блокових шифрів, створених на основі структури "квадрат".

Відомо [5], що кількість можливих перестановок n елементів складає:

$$P_n = n! .$$

Тому, чим більше елементів переставляється, тим більше можливих варіантів перестановок. Якщо правило перестановки буде залежати від секретного ключа, то виникає можливість підвищення стійкості шифрування інформації за рахунок саме реалізації перестановок елементів в межах усього повідомлення, а не його блоку обмеженої довжини.

Нехай, наприклад, реалізується NK правил перестановок, які залежать від секретного ключа K. Тоді зловмиснику потрібно додатково проаналізувати NK варіантів шифрування, порівняно з аналізом шифрування без використання перестановок блоків у межах всього повідомлення.

Відомі алгоритми, що реалізують певні правила перестановки n елементів [5-7]. Однак, вони є достатньо складними для великих значень n і не забезпечують випадкового характеру перестановок.

Тому, актуальними є дослідження, спрямовані на розробку методів формування перестановок, які можуть бути використані при побудові криптографічно стійких шифрів.

Мета дослідження: спрощення процедур формування перестановок будь-якої кількості елементів.

Постановка задач дослідження. Нехай є послідовність чисел:

$$N = \{1,2,...,n\}.$$

Задача полягає у виборі з цієї послідовності кожного числа лише один раз випадковим чином.

Вибір кожного числа – це випробування. Якщо випробуванням присвоїти порядкові номери від 0 до n – 1, то сукупність відповідностей номерів випробувань та вибраних чисел буде описувати правило перестановки:

$$\mathrm{P} = \begin{pmatrix} 0, & 1,..., & n-1 \\ p_0, & p_1,..., & p_{n-1} \end{pmatrix}.$$

Задачею генератора перестановок є формування множини правил P, залежно від певних параметрів.

Відомий метод перестановок без повторень [5, 6], який полягає у формуванні всіх можливих перестановок у лексикографічному або антилексикографічному порядку. Тобто кожна наступна перестановка отримується з попередньої шляхом транспозиції – перестановки двох сусідніх елементів – перших або останніх. Цей метод дозволяє отримати всі можливі перестановки. Однак, він має суттєві обмеження.

Формування всього набору можливих перестановок не дає можливості вибрати довільним чином одну – яка забезпечить псевдовипадковий порядок елементів (кожна з перестановок має монотонності). Крім того, метод, заснований на транспозиції елементів, є неприйнятним в криптографії з точки зору часу виконання. Отже, цей метод непридатний для формування правил перестановок.

Іншим методом генерування перестановок є використання генератора послідовності псевдовипадкових чисел (ПВЧ) [7], який формує в заданому діапазоні всі числа без повторень. Такими генераторами є генератор на основі регістра зсуву зі зворотним зв'язком (РЗЗЗ) та лінійний конгруентний генератор. Однак, обмеженням використання генератора на основі РЗЗЗ є значення модуля 2^d, де d – розрядність генератора, в той час як кількість елементів у множині є довільною.

Лінійний конгруентний генератор реалізує обчислення за формулою:

$$x_i := (a \cdot x_{i-1} + c) \bmod m.$$

Значення модуля m лінійного конгруентного генератора є довільним, однак підбір параметрів генератора є досить складною процедурою. Іншим недоліком є те, що не для будь-якого модуля генератор забезпечує псевдовипадковий характер послідовностей, які формуються. Адже відомо, що для того, щоб лінійний конгруентний генератор сформував усі числа (без повторень) на проміжку [0; n – 1], необхідно виконання трьох умов [7]:

1) числа c та m є взаємно простими;

2) $b = a - 1$ є кратним p для кожного простого p, що є дільником m;

3) b кратне 4, якщо m кратне 4.

Дослідження показують, що для більшості значень m лише значення $a = 1$ задовольняє усім трьом умовам, але воно не забезпечує належної стійкості. Підбір цих параметрів вимагає здійснення складних обчислень (наприклад використання алгоритму Евкліда для пошуку взаємнопростих чисел), що призводить до суттєвих витрат часу. Крім того, генератор використовує операцію множення за модулем, яка є досить складною для обчислювальної техніки [7].

Отже, перераховані методи є непридатними для формування правил перестановок блоків, на які розбивається повідомлення при шифруванні. Тому для досягнення мети дослідження потрібно розв'язати такі задачі:

– розробити узагальнений метод формування правил перестановок;

– сформулювати рекомендації щодо реалізації окремих процедур методу формування перестановок.

Узагальнений метод формування перестановок. Нехай кількість чисел, що підлягає перестановці, дорівнює n і вони пронумеровані від 0 до n – 1 та розташовані в природному порядку. Задача перестановки цих чисел полягає у зміні порядку їх розташування. Ця задача, згідно з методом перестановки, що пропонується, формалізується таким чином:

$$\mathbf{P} = \{\mathbf{N}, \mathbf{G}, I, \mathbf{F}, \boldsymbol{\rho}\},$$

де **N** – набір підпослідовностей, на які розбивається послідовність n чисел.

G – множина функцій формування псевдовипадкових послідовностей:

$$\mathbf{G} = \{G_1, ..., G_4\}.$$

G_1 – функція формування підпослідовностей.

G_2 – функція формування кількості чисел q_i у підпослідовностях.

G_3 – функція формування номеру підпослідовності, для випробування.

G_4 – функція вибору числа (індексу) з підпослідовності.

I –індикатор перестановки;

F – множина правил перестановок;

ϱ– множина перестановок у підпослідовностях.

Послідовність з n чисел розбивається на k підпослідовностей, тобто:

$$\mathbf{N} = \{\mathbf{N}_i\}, \qquad i = 0,1,...,(k-1).$$

При цьому кількість чисел у підпослідовностях може бути як однаковою, так і різною. У випадку однакової кількості чисел у підпослідовностях для їх формування використовується функція G_1. При цьому можливі два варіанти формування підпослідовностей. Перший варіант передбачає завдання кількості підпослідовностей k. Виходячи

зі значення k, обчислюється кількість чисел q_i у підпослідовностях.

Якщо n ділиться на k без остачі, то буде k підпослідовностей з кількістю чисел $q_i = \frac{n}{k}$. Якщо ж результат ділення має остачу, відмінну від нуля, то підпослідовності з 0-ї до (k – 2)-ї складатимуться з $q_i = \left]\frac{n}{k}\right[$ чисел, а (k – 1)-а підпослідовність – з $n - \left]\frac{n}{k}\right[\cdot (k-1)$ чисел, де][означає округлення до більшого цілого числа.

Другий варіант передбачає завдання однакової кількості чисел у підпослідовностях q_i, яка вибирається з діапазону значень:

$$q_i = 2 \div \left]\frac{n}{2}\right[.$$

Отримана кількість підпослідовностей обчислюється за формулою:

$$k = \left]\frac{n}{q_i}\right[.$$

Таким чином, підпослідовності з 0-ї до (k – 2)-ї складатимуться з q_i чисел, а (k – 1)-а підпослідовність – з $n - q_i \cdot (k-1)$ чисел.

Оскільки два описаних варіанти полягають у завданні значення взаємно-обернених величин, то можна зробити висновок, що ці варіанти принципових відмінностей не мають.

У випадку різної кількості чисел у підпослідовностях реалізація функції G_2 передбачає виконання таких дій. Кількість чисел у кожній окремій підпослідовності q_i формується за допомогою деякого генератора ПВЧ. При цьому використовується операція підрахунку кількості сформованих підпослідовностей за таким алгоритмом. На початку кількість послідовностей:

$$k := 0 .$$

Деякому параметру R присвоюється (як початкове) значення кількості чисел n:

$$R_0 := n .$$

На кожному кроці формування підпослідовностей (отримання чергового значення кількості чисел q_i) значення параметра R зменшується на цю кількість:

$$R_{k+1} := R_k - q_i ,$$

Процес формування підпослідовностей триває, поки виконується умова:

$$R > 0 .$$

При цьому кожен крок завершується збільшенням кількості підпослідовностей на одиницю:

$$k := k + 1 .$$

У випадку, якщо $R < 0$, кількість чисел у останній підпослідовності буде дорівнювати R_k.

Незалежно від того, яким чином здійснюється розбиття, перше число кожної підпослідовності обчислюється за формулою:

$$n_{П_i} = \sum_{j=0}^{i-1} q_j ,$$

а останнє – за формулою:

$$n_{O_i} = \sum_{j=0}^{i} q_i - 1 .$$

Порядок вибору підпослідовностей, а також порядок вибору чисел із підпослідовності може бути детермінований або псевдовипадковий. У першому випадку вибір здійснюється із постійним значенням кроку. Вхідними параметрами при цьому є величина кроку a та зміщення b. Номер наступної підпослідовності обчислюється за формулою:

$$n_i = (a \cdot i + b) \bmod k , \ i = 0,1,...,(k-1).$$

У разі псевдовипадкового порядку вибору підпослідовностей значення їх номерів формує деякий генератор ПВЧ.

При детермінованому порядку вибору чисел із підпослідовностей їх номери обчислюються за формулою:

$$n_{ij} = (a_i \cdot j + b_i) \bmod q_i , \qquad i = 0,1,...,(k-1), \quad j = 0,1,...,(q_i - 1). \qquad (1)$$

У разі псевдовипадкового порядку вибору чисел із підпослідовностей їх номери формує деякий генератор ПВЧ.

При застосуванні псевдовипадкового порядку вибору підпослідовностей необхідно використовувати допоміжний параметр – індикатор перестановки. Індикатор перестановки – це ціле число, яке обчислюється для кожної окремої підпослідовності. Його початкове значення дорівнює кількості чисел даної підпослідовності:

$$I_i := q_i .$$

При кожному виборі числа з підпослідовності N_i її індикатор перестановки зменшується на 1. Коли значення індикатора досягає нуля, дана підпослідовність не використовується для вибору чисел. На основі окремих значень індикаторів перестановки формується значення загального індикатора, який визначається за формулою:

$$I = I_0 + I_1 + ... + I_{k-1}.$$

Коли значення індикаторів перестановки усіх підпослідовностей досягнуть нуля, значення загального індикатора також буде дорівнювати нулю і це свідчитиме про завершення процесу формування перестановок. Однак, даний підхід із застосуванням індикатора перестановки прийнятний лише для випадку детермінованого вибору чисел з підпослідовності.

При застосуванні псевдовипадкового порядку вибору чисел із підпослідовностей використання такого підходу неможливе, оскільки він не дає можливості виявити, чи вже було вибрано конкретне число. Тому, в даному випадку, індикатор перестановки являє собою двійкове представлення значення $2^{q_i} - 1$, де q_i – кількість чисел у підпослідовності. Тобто, початкове значення індикатора перестановок – q_i одиниць. При спробі вибору числа з підпослідовності на індикаторний код накладається маска, значення якої обчислюється за формулою:

$$mask := 2^j,$$

де j – порядковий номер числа у підпослідовності.

Результат накладання маски:

$$r := I_K \,\&\, mask.$$

Якщо результат r такої операції дорівнює нулю, це свідчить про те, що дане число вже було вибране, тому воно пропускається. Інакше здійснюється вибір даного числа, а відповідний розряд індикаторного коду встановлюється у значення 0:

$$I_K := I_K \oplus mask.$$

Коли значення індикаторного коду досягає нуля, це свідчить про те, що усі числа даної підпослідовності вибрані. Отже, процес формування перестановок складається з трьох основних етапів:

1) розбиття вхідної послідовності на підпослідовності;
2) вибір підпослідовностей;
3) вибір чисел із підпослідовності.

Виходячи з того, що кожен з них має два можливі варіанти, незалежні один від одного, то існує 8 можливих варіантів процесу перестановки.

Введемо такі позначення: постійний розмір підпослідовностей – C, змінний розмір – V, детермінований порядок вибору (підпослідовностей та чисел) – D, псевдовипадковий – R. Таким чином, маємо отримаємо такі символьні позначення цих варіантів процесу перестановки: CDD, VDD, CRD, VRD, CDR, VDR, CRR, VRR.

Оцінка результатів дослідження. Порівняльний аналіз розробленого методу та відомих методів формування перестановок показує таке. Перевагою запропонованого методу над методом із застосуванням генератора ПВЧ на основі РЗЗЗ є придатність запропонованого методу для формування перестановки не лише 2^d елементів, але довільної кількості елементів, що і вимагається у постановці задач.

На відміну від методу із застосуванням лінійного конгруентного генератора, запропонований метод немає обмежень на вхідні параметри. Вибір будь-яких вхідних параметрів забезпечує формування псевдовипадкової перестановки довільної кількості елементів без повторень, а також немає потреби виконувати складні обчислення для підбору релевантних вхідних параметрів. Крім того, запропонований метод не передбачає виконання операції множення.

Так, наприклад, у формулі (1) множення зводиться до виконання додавання значення a_i до попереднього результату за модулем q_i. Тому розроблений метод є більш прийнятним для обчислювальної техніки.

Порівняння запропонованого методу із лексикографічним методом не має сенсу, оскільки останній взагалі не дає можливості сформувати одну окремо взяту перестановку, яка забезпечує псевдовипадковий порядок елементів, а тому не дає змоги досягти мети, сформульованої в постановці задач дослідження.

Для оцінки випадковості послідовності чисел довільного обсягу без повторень використовуються такі статистичні характеристики: коефіцієнт кореляції з вихідною послідовністю (з числами у природному порядку), а також коефіцієнти автокореляції першого та другого порядків [7-8]. Значення коефіцієнту кореляції отриманої послідовності із початковою послідовністю дозволяє оцінити рівень залежності між двома множинами

(для забезпечення псевдовипадковості перестановки цей рівень повинен бути мінімальним).

Значення ж коефіцієнтів автокореляції першого та другого порядків дають можливість оцінити залежності всередині власне отриманої після перестановки послідовності, а саме – оцінити рівень залежності кожного наступного елемента від попередніх (цей рівень також повинен бути щонайнижчим) [8].

Тому для кожного з наведених варіантів формування перестановок були отримані вказані вище коефіцієнти. Для кожного варіанту формування процесу перестановки було вибрано декілька значень розміру вхідної послідовності (32, 50, 64, 100, 128, 200, 256, 300) та вхідних параметрів генераторів, необхідних для того чи іншого варіанту.

На основі отриманих значень для кожного з варіантів отримане усереднене значення, яке обчислене як середнє арифметичне абсолютних значень отриманих коефіцієнтів. Ці усереднені значення для згенерованих тестових послідовностей наведені в табл. 1.

Таблиця 1

Статистичні характеристики режимів формування перестановок

Режим	**Усереднений коефіцієнт кореляції з вхідною множиною**	**Усереднений коефіцієнт автокореляції першого порядку**	**Усереднений коефіцієнт автокореляції другого порядку**
CDD	0,133	0,326	0,246
VDD	0,269	0,112	0,275
CRD	0,162	0,271	0,204
VRD	0,161	0,116	0,221
CDR	0,072	0,275	0,166
VDR	0,174	0,045	0,231
CRR	0,141	0,164	0,202
VRR	0,198	0,116	0,093

Найбільш близькою до випадкової вважається така послідовність, яка має значення цих коефіцієнтів близьким до нуля [7]. Тому, за отриманими даними, можна зробити висновок, що найкращі статистичні характеристики мають варіанти із псевдовипадковими порядками вибору підпослідовностей та чисел (найнижчі коефіцієнти кореляції).

Висновки. Наведений огляд існуючих методів генерування перестановок показав, що одні методи не забезпечують формування довільної перестановки із псевдовипадковим порядком чисел, інші – непридатні для довільної кількості чисел або не забезпечують псевдовипадкового порядку чисел.

Тобто існуючі методи неможливо використати для формування правил перестановок блоків, на які розбивається повідомлення при шифруванні.

Особливістю запропонованого методу є перестановка чисел у межах всієї опорної множини із забезпеченням їх псевдовипадкового порядку. Використання такого підходу забезпечує підвищення криптографічної стійкості шифрування за рахунок збільшення кількості можливих перестановок.

Розроблений метод може мати 8 варіантів реалізації, які відрізняються характером розміру підпослідовностей (фіксований або змінний), а також порядком вибору підпослідовностей та чисел з окремої підпослідовності (детермінований або псевдовипадковий).

З точки зору випадковості сформованих підпослідовностей найкращими є варіанти із псевдовипадковим порядком вибору.

ЛІТЕРАТУРА

[1]. Шеннон К. Работы по теории информации и кибернетике. — М.: Изд. иностр. лит., 1963. — 830 с.

[2]. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002 – 816 с.

[3]. Ковалевский В. Криптографические методы. – М.: "Компьютер Пресс", 1993 – 236 с.

[4]. Баричев С. Г., Гончаров В. В. Стандарт AES. Алгоритм Rijndael. – М.: "Горячая линия – Телеком", 2002 – с. 30-35.

[5]. Липский В. Комбинаторика для программистов. – М.: "Мир", 1988 – 200 с.

[6]. Виленкин Н. Я. Индукция. Комбинаторика. – М.: "Просвещение", 1976 – 48 с.

[7]. Кнут Д. Искусство программирования. Часть 2. – М.: "Мир", 1976 – 788 с.

[8]. Орлов А.И. Прикладная статистика. Учебник. / А. И. Орлов. – М.: Издательство «Экзамен», 2004 – 656 с.

REFERENCES

[1]. Shannon, C. (1963) Works About Information Theory and Cybernetics. Moscow: Foreign Literature Edition.
[2]. Schneier, B. (2002) Applied Cryptography. Moscow: Triumph.
[3]. Kovalevskiy, V. (1993) Cryptographic methods. Moscow: Compuer-Press.
[4]. Barichev, S. (2002) AES Standard. Rijndael Algorithm. Moscow: Hot Line – Telecom.
[5]. Lipskiy, V. (1988) Combinatory for Programmers. Moscow: Mir.
[6]. Vilenkin, N. (1976) Induction. Combinatory. Moscow: Prosveshchenie.
[7]. Knuth, D. (1976) The Art of Computer Programming. Part 2. Moscow: Mir.
[8]. Orlov, A. (2004) Applied statistics. Moscow: Ekzamen.

МЕТОД ФОРМИРОВАНИЯ ПЕРЕСТАНОВОК ПРОИЗВОЛЬНОГО КОЛИЧЕСТВА ЭЛЕМЕНТОВ

Базовыми операциями любого алгоритма шифрования являются замена и перестановка, потому для построения криптографически стойкого шифра нужен надёжный генератор перестановок. Современные шифры осуществляют перестановки только в пределах отдельного блока, а не блоков в пределах всего сообщения, что не позволяет повысить стойкость. Кроме того, существующие методы формирования перестановок или вообще не дают возможности сформировать отдельную псевдослучайную перестановку, или имеют ограничения на количества элементов опорного множества, или не обеспечивают псевдослучайного характера перестановок и являются сложными с точки зрения реализации. Разработан метод, который обеспечивает формирования псевдослучайной перестановки произвольного количества элементов и является довольно простым в реализации за счёт отсутствия сложных вычислений. Метод имеет восемь вариантов, которые отличаются статистическими характеристиками оценки псевдослучайности. Приведён алгоритм формирования перестановок, математическая модель и оценки сравнения разработанного метода с существующими.

Ключевые слова: перестановка, псевдослучайная перестановка, опорное множество, количество элементов, сложность реализации, статистические характеристики.

THE METHOD OF PERMUTATIONS GENERATING FOR AN ARBITRARY QUANTITY OF ELEMENTS

Every ciphering algorithm is based on two operations: substitution and permutation. So it is required to have a reliable permutations generator to construct a cryptographically strong cipher. The modern ciphers perform permutations only inside one separate block but not for the blocks among the whole message and this does not allow increasing the strength. Moreover the existing methods of permutations generating either do not allow generating a single pseudorandom permutation or having restrictions on the quantity of elements of the base set or do not provide the pseudorandom format of the permutations and they are difficult in the point of view of implementation. The developed method provides generating of a single pseudorandom permutation of an arbitrary quantity of elements and it is quite easy in implementation due to absence of complex computations. The method has eight variants which differ with the statistical characteristics of pseudorandomnicity evaluation. The algorithm of permutations generating, the mathematical model and the evaluation of comparison between the developed and existing methods are shown in this article.

Index Terms: permutation, pseudorandom permutation, base set, quantity of elements, complexity of implementation, statistical characteristics.

Лужецький Володимир Андрійович, доктор технічних наук, професор, завідувач кафедри захисту інформації Вінницького національного технічного університету).
E-mail: lva_zi@mail.ru
Лужецкий Владимир Андреевич, доктор технических наук, профессор, заведующий кафедрой защиты информации Винницкого национального технического университета.
Volodymyr Luzhetskiy, PhD, Head of Department of Information Protection, Vinnitsya National Technical University (Vinnistya, Ukraine).

Горбенко Іван Сергійович, аспірант кафедри захисту інформації Вінницького національного технічного університету.
E-mail: milyaga89@gmail.com
Горбенко Иван Сергеевич, аспирант кафедры защиты информации Винницкого национального технического университета.
Ivan Gorbenko, postgraduate, Department of Information Protection, Vinnitsya National Technical University (Vinnistya, Ukraine).