УДК 004.056

Недолько В.С
Лужецький В.А

МЕТОД БЛОКОВОГО ШИФРУВАННЯ НА ОСНОВІ ПЕРЕСТАНОВОК

Вінницький національний технічний університет

Анотіція. *Запропоновано метод блокового шифрування з використанням перестановок, який базується на двовимірному представленні даних.*
Ключові слова: блоковий шифр, двовимірне представлення, перестановки.

Abstract. *The method of block encryption using permutations, based on two-dimensional view.*
Keywords: block cipher, a two-dimensional representation reshuffle.

Вступ

Існує велика кількість блокових шифрів, які відрізняються наборами виконуваних операцій, але ці операції реалізують два основних перетворення: перестановки та заміни елементів повідомлення, що зашифровується[1]. Найбільших результатів досягнуто в реалізації замін, тому більшість відомих на цей час блокових шифрів реалізується з використанням достатньо складних замін, тоді як перестановки, використовувані в блокових шифрах, є достатньо простими і незалежними від секретного ключа[2]. Тобто в сучасних блокових шифрах не використовуються потенційні можливості підвищення стійкості шифрування за рахунок використання складних перестановок, що залежать від секретного ключа.

Відомо, що кількість можливих перестановок N елементів дорівнює N!. Наприклад, якщо повідомлення складається з 1000 елементів, то кількість можливих перетворень дорівнює 1000!. Це забезпечує достатньо високий рівень стійкості блокового шифрування побудованого лише на операціях перестановки елементів.

Результати дослідження

У роботі презентується метод блокового шифрування з використанням перестановок, який базується на переході від одновимірного представлення до двовимірного. Модель перетворень, що реалізуються при шифруванні, наведено на рис.1.

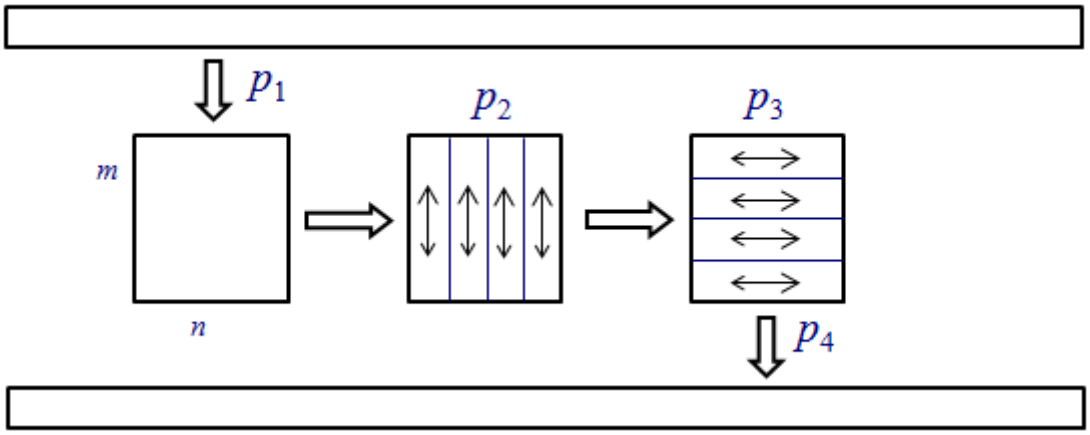

Рисунок 1 – Модель процесу зашифрування

Тут блок відкритого тексту представляється у вигляд масиву розмірністю $m \cdot n$, з використанням перетворення $p1$. Наступним кроком є перестановки елементів у стовбцях масиву шляхом реалізації перетворень p2. Після цього відбувається перестановка елементів у рядках масиву на основі перетворення p3.

Останнім кроком зашифрування є перетворення p4 двовимірного масиву у лінійну форму подання даних. Таким чином процес зашифрування даних є композицією перетворень:

$$P = p1 * p2 * p3 * p4.$$

Змісти кожного перетворення визначається відповідною складовою секретного ключа. Перетворення p1 передбачає формування двовимірного масиву розмірністю mxn, при цьому m та n є змінними, що визначаються секретним ключем. Крім того, перетворення p1 визначає порядок заповнення масиву елементами. Це заповнення може відбуватися або в детермінований спосіб по рядках (стовпцях), або в псевдовипадковий спосіб, що описується відповідними формулами для обчислень номерів позицій елементів в масиві. Отже складовими секретного ключа, що визначає правило $p1$, є значення m і n, та параметри a і b, що входять до формули, за якою обчислюються номери елементів масиву.

Перетворення $p2$ - це набір правил для перестановок елементів у кожному із стовпців. Кожне із цих правил характеризується двома параметрами. Таким чином, кількість складових секретного ключа, що визначає $p2$, дорівнює $2m$.

Перетворення $p3$ - це набір правил аналогічних до $p2$, тільки вони застосовуються до елементів рядків. Кількість складових секретного ключа для цього набору правил дорівнює $2n$.

Перетворення p4 описується двома параметрами. Таким чином, секретний ключ має такі складові:

m,n, a, b, c1, d1…cn, dn, g1, h1….gm, hm, p, q.

для p1 для p2 для p3 для p4

Усі перетворення передбачають виконання однакової послідовності операцій, зчитування елемента даних, обчислення номера позиції елемента в масиві, запис елемента в масив.

Кількість таких операцій для кожного перетворення дорівнює $m \cdot n$. Отже, час зашифрування обчислюється за формулою.

$$T_{\text{заш}} = 4m \cdot n\left(t_{\text{зчит}} + t_{\text{о.н.е}} + t_{\text{зап}}\right),$$

де $t_{\text{зчит}}$ - час зчитування елементів даних з масиву,

$t_{\text{о.н.е}}$ - час обчислення номера позиції елементів в масиві,

$t_{\text{зап}}$ - час запису елемента даних в массив.

Висновки

Запропонований метод блокового шифрування відрізняється від відомих методів виконанням лише перестановок елементів без виконання підстановок. Стійкість такого методу буде достатньою тільки тоді коли переставляється велика кількість елементів, тому цей метод пропонується використовувати для шифрування великих обсягів даних.

Використання простих операцій для реалізацій перестановок забезпечує даному методу найменшу алгоритмічну складність порівняно з відомими методами шифрування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. А. А. -Петров - М.: ДМК, 2000. - 448 с.
2. Жуков А. Е. Легковесная криптография. Часть 1./ Жуков А. Е. // Вопросы кибербезопасности.- № 1(9).- 2015р. – С. 14 26.

Недолько Владислав Станіславович — студент групи 1БС-13б, факультет інформаційних технологій та компютерної інженерій, Вінницький національний технічний університет, Вінниця, e-mail: 15nws@mail.ru

Науковий керівник: ***Лужецький Володимир Андрійович*** — д-р техн. наук, професор, завідувач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Nedolko Vladislav - student group 1BS-13b, faculty of information technology and computer engineers, Vinnytsia National Technical University, Vinnytsia, e-mail: 15nws@mail.ru

Supervisor: ***Luzhetsky Volodymyr*** - Dr. Sc. , Professor, Head of Department of protection informations of Vinnitsa National Technical University. Vinnitsya