Модель блокового шифрування на основі перестановок

Лужецький В.А.[1], Заглада В.І.[2]

[1]Проф., д.т.н., завідувач кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе, 95, м. Вінниця, Україна
[2]Аспірант кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе, 95, м. Вінниця, Україна

***Анотація* — Представлено модель блокового шифрування двовимірних представлень даних на основі перестановок. Обґрунтовано використання блокових шифрів типу "квадрат". Наведено схему роботи шифрування даних. Представлено шифрування та розшифрування двовимірних представлень даних на основі перестановок.**

Ключові слова: блоковий шифр, двовимірне представлення даних, шифрування на основі перестановок.

Model of block encryption based on permutations

Luzhetskyi V.A.[1], Zahlada V.I. [2]

[1] Prof., Head of Information Protection Department, Vinnytsia National Technical University
prosp. Khmelnytske 95, Vinnytsia, Ukraine
[2] Postgraduate of Information Protection Department, Vinnytsia National Technical University
prosp. Khmelnytske 95, Vinnytsia, Ukraine

***Abstract* — Model of two-dimensional block encryption of the data based on permutations has been presented. Application of block ciphers such as "square" has been proved. The diagram of encryption data has been showed. Encrypt and decrypt two-dimensional representations of data based on permutations has been showed Presented.**

Keywords: block cipher, two-dimensional representation of data, encryption based on permutations.

I. Вступ

У сучасному світі одна з найголовніших та важливих речей у житті людини – це інформація. Вона вимагає захисту від нелегального її отримання особами, що не мають прав на доступ до неї. Існує безліч методів та засобів для захисту інформації від неправомірного доступу, але криптографічне закриття інформації є єдиним способом надійного захисту інформації при її зберіганні чи передаванні по лініях зв'язку. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання.

Переважна більшість стійких криптосистем реалізована на основі симетричних блокових шифрів. Алгоритм симетричного блокового шифрування полягає в тому, що відбувається багатократне перетворення блоку вхідних даних з використанням секретного ключа. Користувач чи власник інформації може використовувати один і той самий секретний ключ для зашифрування та розшифрування даних. Симетричні блокові шифри побудовані на основі мереж Фейстеля, SP – мереж, типу "квадрат" [1] та основі арифметичних операцій за модулем [2].

Симетричні блокові шифри типу "квадрат" передбачають представлення блоку даних і секретного ключа у вигляді двовимірного масиву. Криптографічні перетворення можуть виконуватись над окремими байтами масиву, а також над його стовпчиками та рядками [1].

Більшість розроблених блокових шифрів були скомпрометовані і була доведена їх вразливість до зламу. Розробка блокових шифрів типу "квадрат" і використання перестановок дозволить підвищити стійкість до зламу.

У доповіді розглядається один з можливих підходів до блокового шифрування з використанням перестановок, що базується на двовимірному представленні даних і секретних ключів.

II. Основи моделі блокового шифрування на основі перестановок

Особливість перестановки полягає в використанні таких перетворень, які виключають можливість відновлення взаємозв'язку статичних властивостей відкритого та зашифрованого повідомлення. [3]

Дані, що підлягають шифруванню розбиваються на блоки певної довжини:

$$M = m_1, m_2, ..., m_n$$

Секретний ключ K використовується для формування крокових ключів шляхом використання елементів його двовимірного представлення.

На рис. 1 наведено схему шифрування блоку на основі перестановок.

Рисунок 1 – Схема шифрування блоку даних

Значення блоку даних після кожного кроку визначається такими функціями:

$$C_i^{(1)} = f_1(m_i, K_1);$$
$$C_i^{(2)} = f_2(m_i, K_2);$$
$$C_i^{(3)} = f_3(m_i, K_3);$$
$$C_i = f_4(m_i, K_4),$$

де крокові ключі формуються наступним чином:

$$K_1 = g_1(K),$$
$$K_2 = g_2(K),$$
$$K_3 = g_3(K),$$
$$K_4 = g_4(K).$$

З урахуванням цього маємо таку функцію зашифрування блоку даних:

$$C_i = f_4(f_3(f_2(f_1(m_i, K_i), K_2), K_3), K_4)$$

Перед початком кроку, відбувається формування крокового ключа K_n (n = 1, 2, 3, 4) за правилом $g_n(\cdot)$. Крокоий ключ формується у вигляді бітового масиву. Відповідно до сформованого крокового ключа, блок даних формується у вигляді байтового масиву даних розмірності (i x j) та має вигляд:

$$\begin{bmatrix} s_{0,0}, s_{0,1}, \ldots, s_{0,j} \\ s_{1,0}, s_{1,1}, \ldots, s_{0,j} \\ \cdots \\ s_{i,0}, s_{i,1}, \ldots, s_{i,j} \end{bmatrix},$$

де $s_{i,j}$ - елемент блоку даних в i–му рядку та j-му стовбці масиву.

Шифрування блоку даних відбувається шляхом перестановок. Крокові ключі відповідають за перестановки елементів масиву даних.

Відбувається зчитування i-го рядка масиву крокового ключа. Отримане значення є двійковим представленням числа. Дані переводяться з двійкового представлення в десяткове. Значення яке було отримане, є індексом рядка над яким буде виконана перестановка з i-м рядком масиву даних. Якщо отриманий індекс дорівнює індексу i-го рядка, то перестановка не відбувається.

Після закінчення перестановок рядків масиву, виконуються перестановки стовбців масиву. Відбувається зчитування j-того стовпця крокового ключа. Отриманні дані переводяться з двійкового представлення в десяткове. Значення, яке було отримане, є індексом стовпця, над яким буде виконана перестановка з j-тим стовпцем масиву даних. Якщо отриманий індекс дорівнює індексу j-го стовпця, то перестановка не відбувається. .

При розшифруванні даних спочатку відбувається перестановка за стовбцями, а далі - перестановка рядків. Крокові ключі генеруються відповідним чином.

III. Висновки

Використання даної моделі шифрування дозволяє підвищити стійкість до зламу за рахунок використання шифрування типу “квадрат”, оскільки відомі дослідження свідчать про високу стійкість цього класу блокових шифрів, а також за рахунок формування різних розмірностей двовимірного масиву даних та ключа для кожного кроку. За рахунок перестановок маскуються взаємозв'язки між відкритим текстом, шифротекстом і ключем.

[1] Панасенко С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.

[2] Daemen J. Block ciphers based on modular arithmetic / J. Daemen, R. Govaerts // In Proceedings of the 3rd symposium on State and Progress of Research in Cryptography, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, 1993. – pp. 80-89.

[3] Kam J. Structured design of substitution-permutation encryption networks / J. Kam, G. Davida // IEEE Transactions on Computers. – 1979. – Vol. 28, №10. – P. 747.