Шифри перестановок блоків змінної довжини

Лужецький В.А.[1], Горбенко І.С.[2]

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

[2]Аспірант кафедри захисту інформації, Вінницький національний технічний університет, вул. Хмельницьке шосе 95, м. Вінниця, Україна, milyaga89@gmail.com

***Анотація* — Сучасні шифри здійснюють фіксовану перестановку лише в межах окремого блоку. Можна здійснювати перестановку блоків у межах всього повідомлення. Однак, якщо довжина блоків фіксована, початкові та кінцеві позиції блоків після перестановки залишаються відомими. Для усунення цього недоліку пропонується здійснювати розбиття повідомлення на блоки змінної довжини. Для цього розроблено методи перестановок блоків змінної довжини, запропоновано підходи до формування псевдовипадкових значень довжин блоків, отримано оцінки розроблених методів шифрування та формування значень довжин блоків.**

Ключові слова:* *перестановка, блоки змінної довжини, відкрите повідомлення, шифротекст, генератор псевдовипадкових чисел.

Permutation ciphers with variable length blocks

Luzhetskiy V.A.[1], Gorbenko I.S.[2]

[1]Prof., Head of Department of Information Protection, Vinnitsya National Technical University Khmelnitskiy road. str., 95, Vinnitsya, Ukraine, lva_zi@mail.ru

[2] Post-graduate of Department of Information Protection, Vinnitsya National Technical University Khmelnitskiy road. str., 95, Vinnitsya, Ukraine, milyaga89@gmail.com

***Abstract* — Modern block ciphers perform fixed permutation only inside a separate block. It is possible to perform blocks permutation of the entire message. But for fixed length blocks the beginning and ending position of each block remains known after permutation. To remove this issue it is offered to divide the message to the blocks of variable length. Developed permutation methods for variable length blocks, offered approaches to generating values of the blocks length, obtained the evaluations of the developed ciphering methods and generating blocks length methods.**

***Keywords:* *permutation, variable length blocks, open message, ciphertext, pseudorandom number generator*.**

I. Вступ

Сучасні блокові шифри здійснюють перестановку лише в межах окремого блоку. Перестановка є фіксованою (не залежить від секретного ключа), тобто можливість операції перестановки використовується не повною мірою.

У [1] запропоновано метод формування псевдовипадкових (залежних від ключа) перестановок блоків у межах всього повідомлення. Однак, відомі шифри здійснюють розбиття повідомлення на блоки фіксованої довжини. Отже, початкові та кінцеві позиції блоків є відомими навіть після перестановки блоків.

Для усунення цього недоліку пропонується розбивати повідомлення на блоки змінної довжини. Тому дослідження включає розробку методів шифрування на основі перестановки блоків та підходів до формування довжин блоків псевдовипадковим чином.

II. РОЗРОБКА МЕТОДІВ ШИФРУВАННЯ

Нехай повідомлення M розбите на N блоків:

$$M = \{m_0 \,||\, m_1 \,||\, ... \,||\, m_{N-1}\}.$$

Запропоновані шифри перестановок базуються на двох основних операціях:

1) зчитування відкритого повідомлення (R);

2) запис шифротексту (W).

Зчитування і запис можуть здійснюватись у природному (U), детермінованому (D) або псевдовипадковому (P) порядку. Тому можливі методи шифрування: R_UW_D, R_DW_U, R_UW_P, R_PW_U, R_DW_D, R_DW_P, R_PW_D, R_PW_P.

В методі R_UW_D формування шифротексту починається з 0-го блоку відкритого повідомлення:

$$C_0 := m_0.$$

Після цього – за правилом:

$$C_i = \begin{cases} C_{i-1} \,||\, m_i, \text{ якщо } i \text{ парне} \\ m_i \,||\, C_{i-1}, \text{ якщо } i \text{ непарне} \end{cases}$$

Остаточний шифротекст має вигляд:

Метод R_DW_U здійснює формування шифротексту за правилом: $C_i := C_{i-1} \,||\, m_j$,

$$j = \begin{cases} \dfrac{i}{2}, \text{ якщо } i \text{ парне} \\ N - \dfrac{i+1}{2}, \text{ якщо } i \text{ непарне} \end{cases}.$$

Обидва методи забезпечують детермінований порядок блоків після перестановки, оскільки ознакою

визначення адреси зчитування блоку або запису блоку є індекс блоку відкритого повідомлення. Отже, криптографічна стійкість визначається лише правилом вибору довжин блоків. Для забезпечення псевдовипадкового порядку блоків після перестановки пропонується ввести правило формування ознаки. Для цього може бути використаний генератор на основі регістра зсуву зі зворотним зв'язком. На кожному кроці зчитується значення s_i виходу генератора:

$$s_i = \{0,1\},$$

яке є ознакою. Тому при записі шифротексту у псевдовипадковому порядку правило формування шифротексту має вигляд:

$$C_i = \begin{cases} C_{i-1} \parallel m_i, \text{якщо } s_i = 0 \\ m_i \parallel C_{i-1}, \quad \text{якщо } s_i = 1 \end{cases}$$

а при псевдовипадковому порядку зчитування відкритого повідомлення індекс блоку відкритого повідомлення, який необхідно зчитати, визначається так:

$$j = \begin{cases} \dfrac{i}{2}, \text{ якщо } s_i = 0 \\ N - \dfrac{i+1}{2}, \text{ якщо } s_i = 1 \end{cases}$$

III. ФОРМУВАННЯ ДОВЖИН БЛОКІВ

Нехай кількість значень довжини блоків Q.

Вибір значень довжин блоків детермінований або псевдовипадковий. Детермінований вибір має недоліки, оскільки після кожних Q блоків значення повторюватимуться. Тому доцільно використовувати псевдовипадковий вибір. Для цього генератор повинен формувати значення в діапазоні [0; Q – 1]. Доцільно використовувати генератор на основі РЗЗЗ, (простий у реалізації, має високу швидкість). Він формує послідовність двійкових символів, тому кількість символів, необхідна для кодування Q значень:

$$k = \left]\log_2 Q\right[+ 1.$$

Послідовність двійкових символів:

$$P = p_0, p_1, p_2, \ldots, \text{ де } p_i = \{0,1\}.$$

Почергово вибираються групи з k символів:

$g_0 = \{p_0, p_1, \ldots, p_{k-1}\}$, $g_1 = \{p_k, p_{k+1}, \ldots, p_{2k-1}\}$, і т.д.

Кожній групі, ставиться у відповідність число, яке і визначає код значення довжини блоку:

$$l_i = \sum_{j=0}^{k-1} g_{i,j} \cdot 2^j.$$

Інший варіант – формування кодів значень на основі станів генератора РЗЗЗ, де його стан S_i з d розрядів, який розглядається як число:

$$S_i = \{s_{i,j}\}, \ j = 0,1,\ldots,d-1.$$

З S_i обирається група з k молодших розрядів:

$$g_i = \{s_{i,(d-k+1)}, s_{i,(d-k+2)}, s_{i,(d-1)}\},$$

на її основі, аналогічно до попереднього варіанту, формується код значення довжини блоку l_i.

Після цього обирається група з наступних k розрядів. Якщо d кратне k, на основі одного стану генератора буде сформовано $\dfrac{d}{k}$ кодів значень довжини блоку. Якщо d не кратне k, тоді на основі одного стану формується $\left]\dfrac{d}{k}\right[$ кодів значень довжини блоку, а залишкова кількість розрядів r складає $d - \left]\dfrac{d}{k}\right[$. Потім формується новий стан генератора s_{i+1}. З нього обирається ($k - r$) молодших розрядів, які об'єднуються із залишковими r розрядами з попереднього стану:

$$g_i = \{s_{(i+1),(d-r+1)}, \ldots, s_{(i+1),(d-1)}, s_{i,0}, \ldots, s_{i,(r-1)}\}.$$

У 1-му варіанті використовується генератор на основі РЗЗЗ розрядністю d, його період складає:

$$T_0 = 2^d - 1.$$

Для формування одного значення довжини блоку обирається k розрядів. Отже, період складає:

$$T_1 = \frac{HCK(k, T_0)}{k}.$$

Якщо k та T_0 взаємно прості, то період складає:

$$T_1 = \frac{k \cdot T_0}{k} = T_0 = 2^d - 1.$$

У 2-му варіанті використовуються стани генератора, а для формування окремих кодів значень довжини блоку можуть використовуватися розряди двох суміжних станів, тому період складає:

$$T_2 = HCK(T_0, k).$$

Якщо T_0 та k – взаємно прості, період складає:

$$T_2 = T_0 \cdot k = (2^d - 1) \cdot k.$$

Отже, для забезпечення більшого періоду, доцільніше використовувати 2-й варіант правил вибору значень довжини блоків, де розрядність d та значення періоду не кратні кількості розрядів k.

[1] Лужецький В.А. Метод формування перестановок довільної кількості елементів / В.А.Лужецький, І.С.Горбенко // Захист інформації. – 2013. – №3 – С.262-267.

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

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

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

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