УДК 004.056.055

Лужецький В. А.
Бевзюк А. М.

БЛОКОВИЙ ШИФР З ВИКОРИСТАННЯМ ДВОВИМІРНОЇ МОДЕЛІ ДАНИХ

Вінницький національний технічний університет

Анотація

В роботі запропоновано модель блокового шифру з використанням двовимірної моделі даних, особливістю якого є реалізація перестановок елементів даних при перетворенні одновимірного блоку даних у двовимірний масив та навпаки і перестановки елементів двовимірного масиву шляхом циклічного зсуву елементів рядків та стовпчиків.

Ключові слова: *блоковий шифр, двовимірна модель даних, перестановки.*

Abstract

The paper presents a model of block cipher using two-dimensional data model feature of which is the implementation of permutation of data elements while transforming one-dimensional data block in a two-dimensional array and back and reshuffle two-dimensional array of elements by cyclic shift elements rows and columns.

Keywords: *block code, two-dimensional model data, reshuffle.*

Вступ

Традиційний підхід до побудови комп'ютерних шифрів базується на використанні одновимірної моделі даних і секретного ключа. Однак, для представлення математичних об'єктів використовуються багатовимірні моделі (комплексні числа, кватерніони, матриці, векторні простори та інше) [1].

Тому існують потенційні можливості для реалізації інших підходів щодо побудови блокових шифрів. Найвідомішим є стандарт блокового шифру AES, який базується на двовимірній моделі даних і секретного ключа.

Відомо [2, 3], що будь-який шифр може бути побудований з використанням двох перетворень: замін та перестановок елементів даних, що шифруються. В усіх відомих блокових шифрах стійкість шифрування в основному забезпечується за рахунок стійкості процедури заміни. Тоді як можливості забезпечення стійкості за рахунок використання перестановок елементів використовуються не повною мірою.

Виходячи з цього в роботі пропонується один з можливих варіантів ефективної реалізації перестановок елементів даних, який базується на переході від одновимірного представлення даних до двовимірного.

Результати дослідження

Метод зашифрування даних, що пропонується, передбачає реалізацію таких перетворень:

1) формування двовимірного масиву даних з одновимірного блоку даних (перетворення P_1);
2) циклічний зсув елементів рядків масиву (перетворення P_2);
3) циклічний зсув елементів стовпців масиву (перетворення P_3);
4) формування одновимірного блоку зашифрованих даних з двовимірного масиву (перетворення P_4).

Повідомлення **M**, що підлягає зашифруванню, розбивається на блоки різної довжини **M** = {M_0, M_1, ..., M_{n-1}}. При цьому, довжина блоку визначається секретним ключем і дорівнює добутку розмірності двовимірної матриці $(k \cdot l)$.

Для зашифрування кожного блоку даних використовується окремий секретний ключ, який формується з початкового секретного ключа процедурою розгортання секретного ключа.

Перетворення P_1 полягає у реалізації певного маршруту заповнення двовимірного масиву. Нехай, двовимірний масив має вигляд:

$$M^2 = \begin{pmatrix} m_{00} & m_{01} & \dots & m_{0(k-1)} \\ m_{10} & m_{11} & \dots & m_{1(k-1)} \\ \dots & \dots & \dots & \dots \\ m_{(l-1)0} & m_{(l-1)1} & \dots & m_{(l-1)(k-1)} \\ S_1 & S_2 & \dots & S_k \end{pmatrix} \begin{matrix} R_1 \\ R_2 \\ \dots \\ R_l \end{matrix}$$

Тут R_i позначає і-й рядок, а S_j – j-й стовпчик.

Перетворення P_2 полягає у реалізації функції $R_i^* = f_c(R_i)$, а перетворення P_3 – функції $S_j^* = g_c(S_j)$.

Перетворення P_4 полягає у реалізації певного маршруту зчитування елементів двовимірного масиву і формуванні одновимірного блоку зашифрованих даних.

Параметри кожного з перетворень визначаються певними складовими секретного ключа.

Операції зчитування, запису і циклічного зсуву елементів і обчислення індексів елементів даних є природними для сучасних мікропроцесорів і тому реалізуються швидко. Отже, запропонований блоковий шифр забезпечує високу швидкість шифрування.

Щоб задовольнити сучасні вимоги до стійкості блокового шифру рекомендується використовувати довжину блоку від 64 до 128 байт.

Розшифрування даних полягає у реалізації таких перетворень:

1) формування двовимірного масиву елементів даних з одновимірного блоку зашифрованих даних (перетворення P_4^{-1});
2) циклічний зсув елементів стовпців масиву (перетворення P_3^{-1});
3) циклічний зсув елементів рядків масиву (перетворення P_2^{-1});
4) формування одновимірного блоку розшифрованих даних з двовимірного масиву (перетворення P_1^{-1}).

Висновки

Стійкість запропонованого блокового шифру визначається оцінкою потенційної кількості можливих перестановок елементів $(k \cdot l)!$ і необхідністю перебору усіх можливих комбінацій довжин блоків відкритого тексту.

Запропонований блоковий шифр доцільно використовувати для шифрування даних великого обсягу.

Перелік використаних джерел

1. Бронштейн И. Н. Справочник по математике для инженеров и учащихся втузов. / Бронштейн И. Н., Семендяев К. А. – 13-е изд., исправленое. – М.: Наука, Гл. ред. физ.-мат. лит., 1986. – 544с.
2. Горбенко І. Д. Прикладна криптологія. Теорія, практика, застосування : підручн. / Горбенко І. Д., Горбенко Ю. І. – Харків : Вид-во "Форт", 2013. – 880 с.
3. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е издание. / Брюс Шнайер. – М.: Дело, 2003. – 524 с.

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

Бевзюк Антон Миколайович - факультет інформаційних технологій та комп'ютерної інженерії, група БС-14б, Вінницький національний технічний університет, м. Вінниця.

Volodymyr A. Luzhetskyy –Doctor Sc. (Eng), Professor, Head of Information Protection Department, Vinnytsia National Technical University, Vinnytsia.

Anton M. Bevziuk – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.