НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Науково-навчальний центр прикладної інформатики

ІНСТИТУТ ІННОВАЦІЙНОЇ ОСВІТИ

ТРАДИЦІЇ ТА НОВІ НАУКОВІ СТРАТЕГІЇ У ЦЕНТРАЛЬНІЙ ТА СХІДНІЙ ЄВРОПІ

МАТЕРІАЛИ
ІІІ Міжнародної науково-практичної конференції

26–27 червня 2020 р.
м. Київ

Київ
Інститут інноваційної освіти
2020

УДК 001(063):378.4 (Укр)
ББК 72я43
Т65

До збірника увійшли матеріали наукових робіт (тези доповідей, статті), надані згідно з вимогами, що були заявлені на конференцію.

Роботи друкуються в авторській редакції, мовою оригіналу.
Автори беруть на себе всю відповідальність за зміст поданих матеріалів.
Претензії до організаторів не приймаються.
При передруку матеріалів посилання обов'язкове.

Т65 **Традиції та нові наукові стратегії у Центральній та Східній Європі :** Матеріали ІІІ Міжнародної науково-практичної конференції (м. Київ, 26–27 червня 2020 р.) / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. – Київ : ГО «Інститут інноваційної освіти», 2020. – 140 с.

Матеріали конференції рекомендуються освітянам, науковцям, викладачам, здобувачам вищої освіти, аспірантам, докторантам, студентам вищих навчальних закладів тощо[1].

Відповідальний редактор: *С.К. Бурма*
Коректор: *П.А. Немкова*

Матеріали видано в авторській редакції.

УДК 001(063):378.4 (Укр)

Підписано до друку 03.07.2020. Формат 60х84/16.
Віддруковано з готового оригінал-макету.
Папір офсетний. Друк цифровий. Гарнітура Charter. Ум. друк. арк. 8,14.
Зам. № 0307/20-9. Тираж 100 прим. Ціна договірна. Виходить змішаними мовами: укр., анг.

Виготівник. ФОП Москвін А.А. Цифрова друкарня «Copy Art».
69095, Запоріжжя, просп. Соборний, 109. Тел.: (061) 708-08-80
Інститут інноваційної освіти: e-mail: novaosvita@gmail.com; сайт: www.novaosvita.com

Видання здійснене за експертної підтримки
Науково-навчального центру прикладної інформатики НАН України
03680, Київ-187, просп. Академіка Глушкова, 40.

[1] *Відповідає п. 12 Порядку присудження наукових ступенів Затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567; п. 28 Постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності»; п. 13 Постанови Кабінету Міністрів України від 12 липня 2004 р. № 882 «Про питання стипендіального забезпечення»*

УДК 004.832

В.В. Редич,
здобувач вищої освіти ступеня магістра
Вінницького національного технічного університету
В.А. Лужецький,
доктор технічних наук, професор, завідувач кафедри захисту інформації
Вінницького національного технічного університету

МЕТОД ШИФРУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ УОЛША

Анотація. Розроблено власний метод шифрування на основі перетворення Уолша. Виконано оцінку швидкості шифрування запропонованого методу.

Ключові слова: кібербезпека, шифрування, перетворення Уолша, швидке перетворення Уолша-Адамара, блокове шифрування, матричні перетворення.

Вступ. Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, хвилювала людський розум з давніх часів.

З метою забезпечення конфіденційності інформації використовують особливий вид перетворень, який має назву «шифрування». Шифрування має на меті приховати змістовну та статистичну залежність між частинами вхідного повідомлення. Шифрувати можна будь-які повідомлення, що мають цінність для відправника або одержувача і можуть бути перехоплені третьою стороною з метою подальшого використання у своїх інтересах. Саме тому з розвитком електронних обчислювальних машин та засобів їх взаємодії також розвивалися методи та засоби збереження конфіденційності інформації.

Недоліком усіх блокових шифрів є те, що вони є повільнішими порівняно з потоковими [2]. Тому особливо актуальною задачею в сучасній криптографії є підвищення швидкості блокового шифрування.

Розробка методу. За основу блокового шифру взято швидке перетворення Уолша-Адамара, впорядковане за Адамаром, та додано декілька модифікацій, адже саме перетворення має декілька недоліків з точки зору криптографії, які необхідно виправити.

По-перше, оскільки основою перетворення є операції додавання та віднімання, то це призводить то того, що можуть виникати переповнення, тобто це може призвести до збільшення розрядності, що є неприпустимо для криптографії.

Тому, для того, щоб усунути цей недолік, пропонується виконувати усі операції в межах перетворення за модулем, тобто:

$$X_x(n) = (H_h(n)\, B_x(n)) mod(m), \quad (1)$$

де m – значення модуля.

По-друге, під час оберненого перетворення необхідно виконати ділення на число, яке дорівнює розмірності вектора, що містить секретні дані, а це може призвести до появи дійсних, а не лише цілих чисел, під час обрахунків, а в межах криптографічних перетворень, усі дії бажано виконувати над цілими числами.

Для того, щоб усі перетворення виконувалися лише над цілими числами, пропонується виконувати ділення за модулем, і виконувати його потрібно в якості останньої операції.

Тобто, після внесення змін у швидке перетворення Уолша-Адамара, впорядкованого за Адамаром, процес зашифрування буде виконуватися за формулою:

$$C(n) = (H_h(n)\, M(n)) mod(m), \quad (2)$$

де $C(n)$ – закрите повідомлення;

$M(n)$ – відкрите повідомлення;

m – значення модуля;

$H_h(n)$- матриця Адамара.

А процес розшифрування виконуватиметься відповідно до формули:

$$M(n) = (H_h(n)\, C(n) mod(m)) \frac{1}{N} mod(m), \quad (3)$$

де $n = \log_2 N$.

Для того, щоб забезпечувалося швидке шифрування, пропонується метод шифрування, в якому використовується матриця Уолша, але для забезпечення стійкості алгоритму пропонується використовувати ще два параметри, які визначатимуть розмірність матриці Уолша та секретної довжини блоків даних, що шифруються. Їх умовно позначимо символами d та N.

Для параметру d, що визначає розрядність даних, що будуть оброблятися, в межах роботи пропонується використовувати такий набір значень:

$$d = \{8;\ 16;\ 24;\ 32\}$$

А для параметру N, що відповідатиме за розмірність матриці Уолша, запропоновано такі значення:

$$N = \{8;\ 16;\ 32;\ 64;\ 128\}$$

Для того, щоб визначати які саме значення обирати для параметрів N та d, запропоновано використовувати генератор псевдовипадкової послідовності.

Таким чином визначення значень параметрів відбуватиметься відповідно до формул:

$$N = f_1(K), \quad (4)$$

$$d = f_2(K), \quad (5)$$

де f_1 та f_2 – функції генерації псевдовипадкових послідовностей;

K – значення секретного ключа.

Розрядність блоку L, що буде зашифровано\розшифровано дорівнює добутку розмірності перетворення та розрядності даних.

$$L = N \cdot n \tag{6}$$

Отже, розрядність блоку L також змінна величина. І на рис. 1, що демонструє структуру повідомлення, видно, що повідомлення розбивається на блоки різної розрядності під час шифрування.

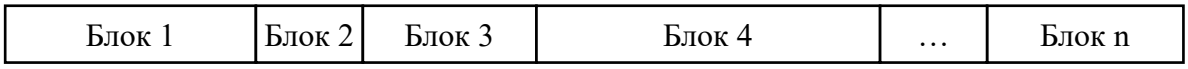

Рисунок 1 – Розбиття повідомлення на блоки різної довжини

У формулах (2) та (3) для обрахунку необхідно мати значення модулю m, яке обчислюється за формулою:

$$m = 2^d - 1 \tag{7}$$

Таким чином було описано алгоритм шифрування даних та описано яким чином отримуються усі необхідні для цього алгоритму параметри.

Висновки. У результаті виконання роботи розроблено блоковий шифр на основі матричних перетворень, який використовує перетворення Уолша-Адамара для пришвидшення процесу шифрування.

Запропоновано метод блокового шифрування, який на відміну від відомих блокових шифрів передбачає використання блоків змінної довжини та перетворення Уолша змінної розмірності і забезпечує підвищення середньої швидкості блокового шифрування.

Список використаних джерел

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А.О. Азарова, В.В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Брассар Ж. Современная криптология / Ж. Брассар. – М.: Полимед, 1999. – 354 с.
3. Ахмед Н. Ортогональные преобразования при обработке цифровых сигналов./ Н. Ахмед , К.Р. Рао.; Пер. с англ. / Под ред. И.Б. Фоменко. – М.: Связь, 1980. – 248 с.
4. Luzhetskiy V. Substitution cipher based on pseudo non-determined gamma generator / V. Luzhetskiy, I. Gorbenko // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 159–163.

V.V. Redych, V.A. Luzhetsky,

Walsh transformation based encryption method.

Summary. Developed own method of encryption based on the Walsh transformation. The encryption speed of the proposed method is estimated.

Keywords: cybersecurity, encryption, Walsh transform, fast Walsh-Hadamard transformation, block encryption, matrix transformations.