КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 519.6 DOI:10.34229/2707-451X.25.1.6

І.А. БАРАНОВ

СИМЕТРИЧНИЙ БЛОЧНИЙ АЛГОРИТМ WBC1 ТА АНАЛІЗ СКЛАДНОСТІ ЙОГО РЕАЛІЗАЦІЇ

Описується симетричний блочний криптографічний алгоритм WBC1. У статті детально розглядається процес шифрування, аналіз складності алгоритму і швидкості виконання. Показана реалізація алгоритму.

Ключові слова: *симетричний блочний криптографічний алгоритм, аналіз складності симетричного блочного криптоалгоритму, аналіз швидкості криптоалгоритму, криптографія, криптографічний алгоритм.*

Вступ. Комп'ютерні мережі на сьогодні набувають все більшого значення для обміну інформацією. Криптографія відіграє життєво важливу роль у безпеці зв'язку в мобільних телефонах, паролів у обчислювальній техніці та навіть інженерії, на відміну від давніх часів, коли криптографія полягала лише у шифруванні та розшифровці повідомлень за допомогою ключів. Одна з найважливіших вимог цих мереж це забезпечення безпечної передачі інформації з одного місця в інше. Криптографія це один з методів, що забезпечує найбільш безпечний спосіб передачі конфіденційної інформації від відправника до передбачуваного отримувача [1]. Існує безліч робіт у цьому напрямку [2–13]. Його основна мета – зробити конфіденційну інформацію нечитабельною для всіх, крім передбачуваного отримувача. Великий внесок у сфері криптографії зробили українські вчені В.К. Задірака та А.М. Кудін у своїх наукових працях [14–24].

Всім відомий стандарт шифрування даних (DES) у даний час застаріває через невеликий розмір ключа в 56 біт [6] та незначний розмір блоків шифрування, у зв'язку з цим Національний інститут стандартів і технологій (NIST) представив блочно-орієнтований симетричний криптографічний алгоритм Advanced Encryption Standard (AES) з метою бути як швидшим, так і більш стійким до криптоаналізу. Блоковий шифр AES має 128, 192 або 256-бітний ключ для шифрування, або розшифровки даних блоками по 128 біт [25–29]. Незважаючи на досить збалансовані характеристики алгоритму AES за критерієм стійкість/ефективність, пошук більш ефективних за цим критерієм симетричних блокових алгоритмів шифрування продовжується [30–36].

Актуальним також є створення алгоритмів шифрування, заснованих на нових важкооборних перетвореннях, один з яких пропонується автором.

1. Алгоритм WBC1. Як відомо, будь-які перетворення кодованих повідомлень можна представити у різних видах: аналітичному, табличному, графічному тощо. Головна ідея алгоритму WBC1 полягає у представленні шифруючого перетворення як перетворення просторових тривимірних координат за допомогою моделі кубіка Рубіка.

WBC1 – це блоковий шифр, який шифрує дані в 32, 64, 216 і 512-бітних блоках. На вході алгоритму вводиться 64, 216 або 512-бітний блок відкритого тексту, а на виході – 32, 64, 216 або 512-бітний блок шифротексту.

WBC1 – це симетричний алгоритм: для шифрування та розшифрування використовуються один і той самий ключ. Ключ повинен мати довжину не менше 64 біт.

Ключ, яким може бути будь-яке 64-бітне число, може бути змінений у будь-який момент часу.

Криптографічна стійкість повністю визначається ключем. Основним будівельним блоком WBC1 є комбінація вертикальних і горизонтальних перестановок, кількість яких прямо пропорційна довжині елементів ключа. Наприклад, якщо розмір блоку, на який розбиваються вхідні дані, становить 32 біта, то число всіх можливих станів дорівнюватиме 215!.

Для ілюстрації уявімо собі переданий текст не на площині паперу або екрані монітора, а в обсязі (в тривимірному просторі). А потім застосуємо алгоритм WBC1.

1.1. Процес шифрування. Процес шифрування полягає у тому, що вихідні дані T розміром n біт розбиваються на блоки, де B_i – блок розміром s біт, $s \in \{32, 64, 216, 512\}$ (рис.1),

$$T = \{B_1, B_2, \dots, B_k\},\ k = \frac{n}{s}$$

і записуються у тривимірний масив (куб) розміром $d \times d \times d$, де d вибирається для розміщення всіх блоків. Наприклад, для 32-розрядного блоку куб може бути $2 \times 2 \times 2$.

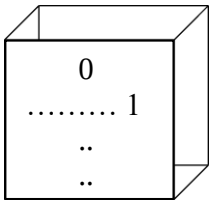

РИС. 1. Блок, що шифрується

Подібно до алгоритму AES, створюється таблиця перестановок P, в якій записано 127 можливих операцій над кубом (тобто обертів його площин і комбінацій). Нехай P містить перестановки $p_1, p_2, \dots, p_{127}$, де кожна перестановка p_i – це операція над кубом.

Після попередніх установок етапи шифрування виконуються у чіткій послідовності.

1. Послідовне сканування елементів ключа K, і в залежності від значення елемента ключа застосовується те чи інше обертання площин куба з можливих 127 комбінацій. Якщо ключ K має довжину k біт, то кожен елемент K_i (де K_i – i-й біт ключа) вибирає операцію O з таблиці P:

$$O = P[K_i].$$

Операція $P[K_i]$ застосовується до куба даних.

2. Після кожного проходу окремого символу ключа реалізується циклічний побітовий зсув (тип циклічного зсуву залежить від реалізації алгоритму, тобто від потужності), рис. 2:

$$B' = F(B, d),$$

де $F(B, d)$ – функція, що виконує циклічний зсув на d біт.

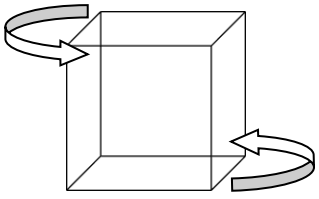

РИС. 2. Циклічний побітовий зсув у блоці

3. Після того, як всі операції будуть застосовані, дані з куба розформовуються у ланцюжок символів.

Процес розшифрування полягає в оберненому проходженні всіх операцій шифрування.

У загальному вигляді цикл перетворень показано на рис. 3.

Враховуючи, що для шифрування та розшифрування WBC1 використовують лише операції перестановки з масива у масив та циклічний побітовий зсув, витрати на пам'ять ідуть лише на створення та роботу з двома тривимірними масивами та бітову операцію. Можна побачити, що слабким місцем алгоритму є обмежене число перестановок (127), але операція циклічного побітового зсуву вирішує цю проблему.

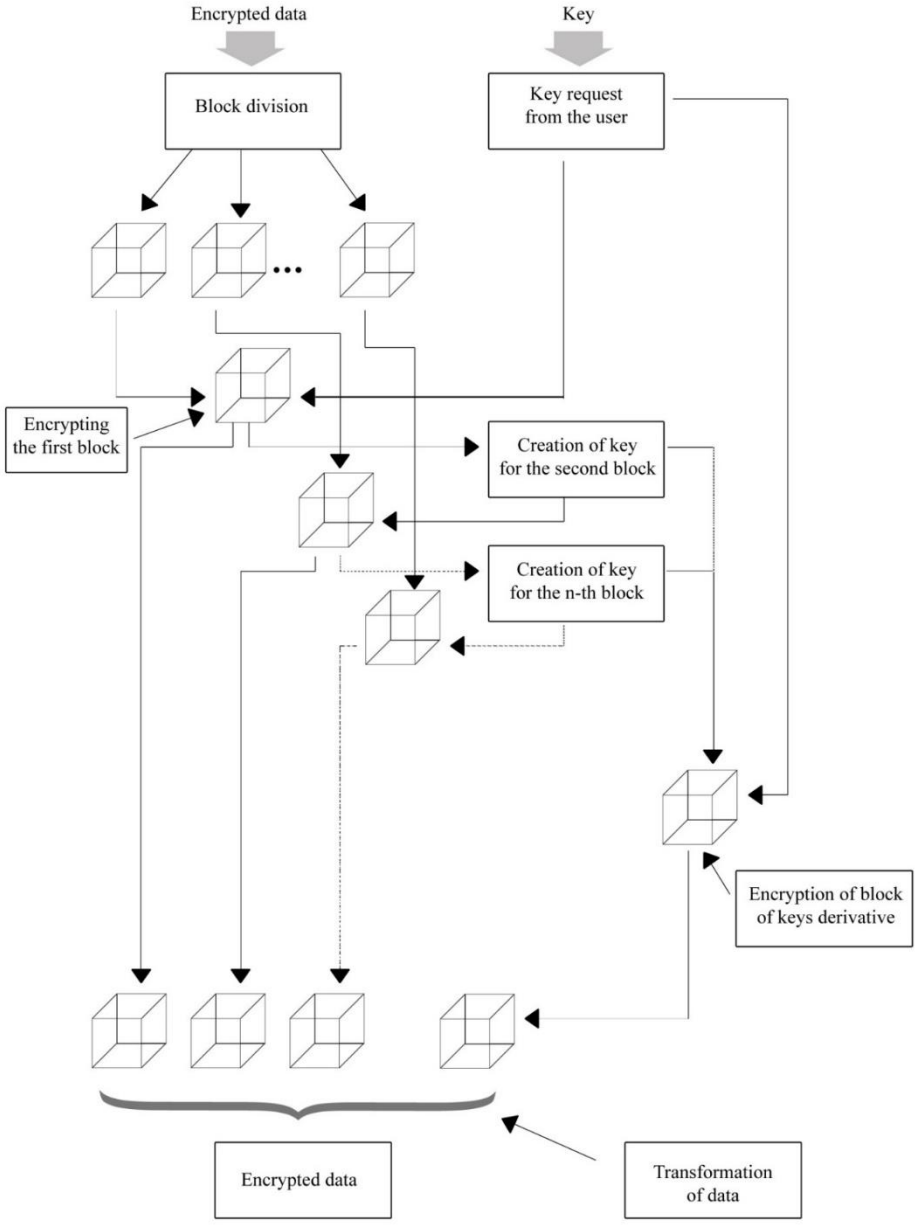

РИС. 3. Схема виконання алгоритму WBC1

1.2. Аналіз складності алгоритму. Щоб оцінити складність алгоритму WBC1, нам потрібно врахувати кілька аспектів: розмір вхідних даних, операції перестановки та зсуву, а також параметри ключа та блоку. Давайте розглянемо кожну з цих частин.

Нехай n – розмір вхідних даних у бітах, s – розмір блоку в бітах, а k – кількість блоків. Тоді

$$k = \frac{n}{s}.$$

Кожен блок даних поміщається в куб розміром $d \times d \times d$, де d вибирається так, щоб розмістити блоки даних. Для простоти припустимо, що куб має розмір $d = \sqrt[3]{s}$. Наприклад, для блоку з 64 біт це може бути куб $4 \times 4 \times 4$, який відповідає $d = 4$.

Таблиця перестановок містить 127 різних операцій, і кожна операція це перестановка над $d \times d \times d$ елементами куба.

Нехай P – таблиця перестановок. Для кожного елемента ключа (нехай довжина ключа дорівнює m) вибирається перестановка та застосовується до куба. Позначимо кількість перестановок у кубі як p. Наприклад, якщо куб має d^3 елементів, то всі можливі перестановки елементів куба $p = d^3!$.

Оскільки перестановки застосовуються до кожного блоку даних, загальна кількість перестановок для одного блоку становитиме $O(p) = O(d^3!)$.

Циклічний зсув це побітова операція, яка виконується за часом, пропорційним розміру блоку $O(s)$.

Опишемо складність алгоритму шифрування. Процес шифрування включає:

1. Розподіл вхідних даних на блоки: це $O\left(\frac{n}{s}\right)$ операції.

2. Для кожного блоку:
   – застосування перестановок – $O(p)$;
   – циклічний побітовий зсув – $O(s)$.

Сумарна складність шифрування для одного блоку складе $O(p) + O(s)$.

Оскільки шифрування виконується для всіх блоків даних, загальна складність шифрування становитиме $O\left(\frac{n}{s} \cdot (d^3! + s)\right)$.

Процес розшифрування включає у себе ті ж операції, що і шифрування, але в зворотному порядку. Тому його складність аналогічно – $O\left(\frac{n}{s} \cdot (d^3! + s)\right)$.

Якщо довжина ключа m, і кожна операція у шифруванні вимагає $O(m)$ для обробки елемента ключа, то загальний час для застосування всіх операцій з ключем становитиме $O\left(m \cdot \frac{n}{s}\right)$.

Але, якщо операція вибору перестановки та її застосування це основна затратна операція, то складність алгоритму в основному визначається кількістю перестановок та розміром блоку.

З огляду на всі вищеперераховані частини, кінцева складність алгоритму WBC1 складе

$$O\left(\frac{n}{s} \cdot (d^3! + s)\right) + O\left(m \cdot \frac{n}{s}\right), \quad (1)$$

де $\frac{n}{s}$ – кількість блоків, $d^3!$ – кількість можливих перестановок елементів куба, $d = \sqrt[3]{s}$ – розмір куба, що відповідає розміру блоку, n – загальний розмір вхідних даних у бітах, s – розмір блоку, m – довжина ключа.

Якщо перестановки це основна витратна операція, то складність буде домінувати від $O(d^3!)$, роблячи її експоненціальною у залежності від розміру блоку в кубі.

1.3. Швидкість виконання алгоритму. Щоб оцінити швидкість виконання алгоритму WBC1, нам потрібно врахувати часову складність різних його етапів і розрахувати фактичний час виконання на основі формули (1). Оскільки точні значення будуть залежати від реалізації і конкретних апаратних характеристик, представимо загальний підхід до розрахунку і приблизні оцінки.

Загальний час виконання алгоритму можна виразити як:

$$T_{total} = T_{split} + T_{encrypt} + T_{decrypt},$$

де T_{split} – час для розділення даних, $T_{encrypt}$ – час для шифрування даних, $T_{decrypt}$ – час для розшифрування даних.

Приклад. Розглянемо на конкретному прикладі розрахунок часу виконання. Для цього нам знадобляться такі дані:

- розмір вхідних даних: n = 1 000 000 біт (приблизно 125 000 блоків по 64 біт);
- розмір блоку: s = 64 біта;
- кількість операцій у залежності від ключа: m = 128.

Розмір куба дорівнює $d = \sqrt[3]{s} = \sqrt[3]{64} = 4$, $d^3! = 64! \approx 1.03 \times 1089$.

Кожен блок даних обробляється з урахуванням всіх перестановок. Складність у застосуванні всіх можливих перестановок до одного блоку $O(d^3!) = O(64!)$.

При обробці всіх блоків даних (де вказано кількість блоків $\frac{n}{s}$) складність $O\left(\frac{n}{s} \cdot (d^3! + s)\right)$.

Тобто,

$$\frac{n}{s} = \frac{1{,}000{,}000}{64} \approx 15{,}625,\ O\left(\frac{n}{s} \cdot (d^3! + s)\right) = O(15{,}625 \cdot (64! + 64)),$$

$$T_{encrypt} = O(15{,}625 \cdot (64! + 64)) \approx O(15{,}625 \cdot 64!).$$

Для операцій, що залежать від ключа:

$$T_{key\_operations} = O\left(m \cdot \frac{n}{s}\right) = O(128 \cdot 15{,}625) = O(2{,}000{,}000).$$

З урахуванням всіх вищеперерахованих факторів:

$$T_{total} = O\left(\frac{n}{s} \cdot d^3!\right) + O\left(m \cdot \frac{n}{s}\right) = O(15{,}625 \cdot 64!) + O(2{,}000{,}000) \approx O(10^{93}).$$

1.4. Попередня оцінка стійкісті до методів криптоаналітичних атак. Алгоритм WBC1 вважається досить стійким до кількох видів криптоаналітичних атак, завдяки своїй унікальній структурі та використовуваним методам. Розглянемо основні методи стійкості:

- *стійкість до перебору (Brute Force),* один з базових і найбільш відомих методів криптоаналізу [35], [38–40], при якому криптоаналітик послідовно перевіряє всі можливі ключі, поки не знайде правильний. Цей метод особливо ефективний проти алгоритмів з короткими ключами, оскільки збільшення довжини ключа експонентно збільшує кількість можливих комбінацій. Алгоритм WBC1 використовує великий простір ключів (наприклад, 64-бітний ключ або більший), а кількість можливих перестановок елементів куба дорівнює $d^3!$, що робить спроби перебору всіх можливих ключів практично неможливими через експоненційне зростання кількості перестановок при збільшенні розміру куба. Це забезпечує високу стійкість до атак повного перебору;
- *диференціальний криптоаналіз* був розроблений Елі Біхамом і Аді Шаміром [34, 35] і це один із найвідоміших методів криптоаналізу, особливо для блочних шифрів. Цей метод дозволяє знаходити залежності між різницями вхідних та вихідних даних, що дає змогу розкрити структуру шифру і в деяких випадках підібрати ключ. Для алгоритму WBC1 диференціальний криптоаналіз є складним завданням через використання тривимірних перестановок і побітових циклічних зсувів, оскільки кожен раунд шифрування залучає великі зміни у вихідних даних у тривимірному просторі. Ці операції сприяють створенню високої ентропії і значного рівня нелінійності, що ускладнює пошук необхідних залежностей між різницями відкритого тексту і шифротексту;
- *лінійний криптоаналіз* [36, 41, 42] – метод криптоаналізу, запропонований Міцуру Мацуї [36] у 1993 році, призначений для атаки на блокові шифри. Основна ідея лінійного криптоаналізу полягає

у пошуку лінійних апроксимацій між відкритим текстом, шифротекстом та ключем, що дозволяє криптоаналітику визначити ключ на основі цих ймовірнісних залежностей. Завдяки використанню складних перестановок і циклічних зсувів, алгоритм WBC1 також добре захищений від лінійного криптоаналізу, оскільки такі операції створюють високий рівень випадковості та нелінійності в процесі шифрування. Це значно ускладнює пошук лінійних залежностей між відкритим текстом, шифротекстом та ключем;

- *атаки на базі сайд-каналів* [43–45] це метод криптоаналізу, при якому зловмисник використовує фізичну інформацію, отримувану під час роботи криптографічного пристрою, для вилучення секретної інформації, такої як ключі шифрування. Ці атаки грунтуються не так на прямому аналізі алгоритму шифрування, як на аналізі додаткових даних, які можна отримати у його виконанні. Використання тривимірного масиву в структурі алгоритму WBC1 може сприяти зниженню ризику деяких типів атак, пов'язаних з витоком інформації (наприклад, атак через аналіз енергоспоживання). Однак це вимагає додаткового тестування для повної впевненості.

Загалом, як відомо, немає досконалої стійкості. Алгоритм WBC1 розроблений для забезпечення високого рівня криптографічної стійкості через поєднання тривимірних перестановок та побітових зсувів, що робить його досить складним для більшості відомих методів криптоаналізу.

1.5. Апробація алгоритму. Алгоритм було реалізовано у двох варіантах: для шифрування тексту і файлу. На рис. 4 показаний скріншот програми для шифрування тексту. У верхньому вікні текст, який потрібно зашифрувати, в нижньому вікні – отриманий зашифрований результат.

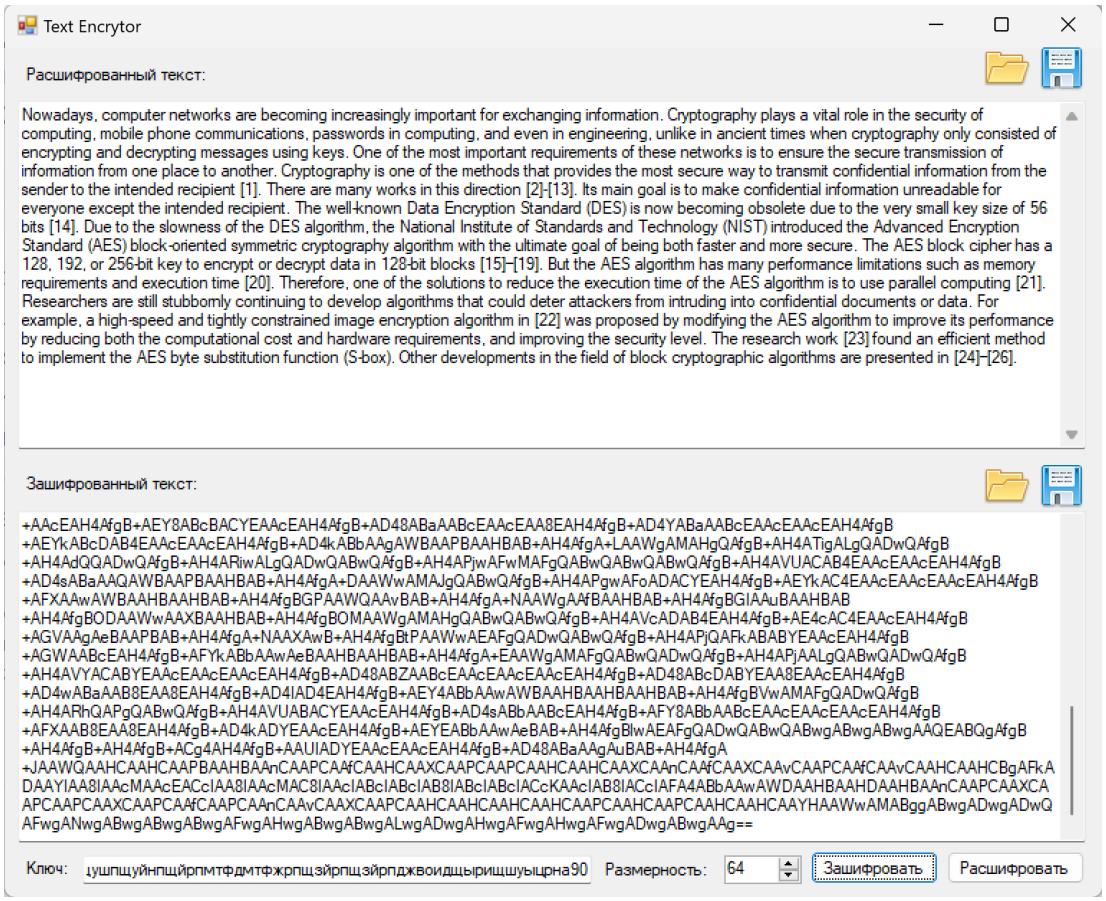

РИС. 4. Скріншот виконаної програми шифрування тексту

Висновки. Основний фактор криптостійкості WBC1 – це кількість можливих перестановок елементів куба. Ця величина дорівнює $d^3!$, де d – розмір куба, що відповідає розміру блоку s. Для s = 64 біт це значення дорівнює 64!, що є надзвичайно великим числом. У зв'язку з експоненціальним збільшенням числа перестановок зі збільшенням s, атаки, засновані на переборі всіх можливих перестановок, стають практично нездійсненними при великих значеннях s. Циклічні побітові зсуви, які застосовуються до блоків даних, додають додатковий рівень складності та перемішування, що ускладнює криптоаналіз.

Потужність алгоритму може збільшуватися у залежності від поставленого завдання. Наприклад, для шифрування документів на домашньому комп'ютері можна обмежитися мінімальними можливостями, такими як: довжина ключа становить до 80 біт, а розмір оброблюваних блоків – 64 біта. Однак цього вже недостатньо для шифрування документів у державних організаціях, і слід використовувати довші ключі (з додатковим процесом розширення ключа). Можливості алгоритму дозволяють реалізувати його як на програмному, так і на апаратному рівні.

Алгоритм WBC1 представляє собою криптографічно стійкий метод шифрування, який забезпечує високий рівень безпеки за рахунок використання складних перестановок і циклічних зсувів. Однак його висока часова складність через експоненціальне зростання перестановок може обмежити його практичне застосування для великих блоків даних і великих обсягів. Для великих обсягів даних слід використовувати методи та алгоритми паралельних та розподілених обчислень для комп’ютерів з паралельною архітектурою, як наприклад в роботах [46, 47].

Якщо врахувати все вищесказане, то можна зробити висновок, що можливості представленого алгоритму досить великі. А можливість збільшення потужності алгоритму робить його гнучким для використання у різних областях та сферах діяльності, пов'язаних з обробкою інформації, що підлягає криптографічному захисту.

Фінансування. Автор не отримував фінансування для проведення досліджень та написання статті.

Список літератури

1. Liu W., Ying B., Yang H., Wang H. Accurate modeling for predicting cryptography overheads on wireless sensor nodes. *11th International Conference on Advanced Communications Technology (ICACT 2009)*. Vol. 2. P. 997–1001. IEEE, 2009.
2. Beutelspacher A. Cryptography. Washington, DC: Mathematical Association of America. 1994. 156 p.
3. Dong X., Qin L., Sun S., Wang X. Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks. *Advances in Cryptology – EUROCRYPT 2022. EUROCRYPT 2022*. Lecture Notes in Computer Science. 2022. Vol. 13277. Springer, Cham. P. 3–13. https://doi.org/10.1007/978-3-031-07082-2_1
4. Advanced Encryption Standard. National Institute of Standards and Technology, Gaithersburg, MD. 2001. https://doi.org/10.6028/NIST.FIPS.197 (звернення: 25.10.2024)
5. Gueron S., Langley A., Lindell Ye. AES-GCM-SIV: Specification and Analysis. *Cryptology ePrint Archive*. 2017. 168 https://eprint.iacr.org/2017/168
6. Anderson R., Biham E., Knudsen L. Serpent: A Proposal for the Advanced Encryption Standard. *In Fast Software Encryption '98*, Springer-Verlag. 1998. P. 222–238.
7. Lai X., Massey J.L. A Proposal for a New Block Encryption Standard. In: Damgård, I.B. (eds) *Advances in Cryptology — EUROCRYPT '90. EUROCRYPT 1990*. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1991. Vol. 473. P. 389–404. https://doi.org/10.1007/3-540-46877-3_35
8. Daemen J., Rijmen V. The Design of Rijndael: AES – Advanced Encryption Standard, Springer-Verlag, 2002. https://doi.org/10.1007/978-3-662-04722-4
9. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976. Vol. 22, No. 6. P. 644–654. https://doi.org/10.1109/TIT.1976.1055638
10. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM 21*. 1978. 2. P. 120–126. https://doi.org/10.1145/359340.359342
11. Baptista M.S. Cryptography with chaos. *Physics Letters A*. 1998. **240** (1-2). P. 50–54. https://doi.org/10.1016/S0375-9601(98)00086-3

12. Wong W., Lee L., Wong K. A modified chaotic cryptographic method. *Computer Physics Communications.* 2001. Vol. 138, Iss. 3. P. 234–236 https://doi.org/10.1016/S0010-4655(01)00220-X
13. Xiang T., Liao X., Tang G., Chen Yo., Wong K. A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A.* 2006. Vol. 349, Iss. 1–4. P. 109–115. https://doi.org/10.1016/j.physleta.2005.02.083
14. Kudin A., Zadiraka V., Shvidchenko I., Bredelev B. Cryptographic and steganografic protocols for cloud systems. *Computer technologies in information security*. Ternopil: "Kart-blansh", 2015. P. 9–41.
15. Zadiraka V. Improving of performance of two-key cryptography systems. *Methods of effective protection of information flows*. Ternopil: Terno-graf, 2014. P. 67–95.
16. Zadiraka V., Shevchuk B. Methods and means of information computer networks security support. *Methods of effective protection of information flows*. Ternopil: Terno-graf, 2014. P. 186–228.
17. Шевчук Б.М., Задірака В.К., Луц Л.В., Луц В.К. Ефективні за швидкодією і точністю кодування методи оперативної обробки, кодування та передачі інформації для побудови бортових засобів мобільних роботів і рухомих систем. *Искусственный интеллект*. 2014. 3. С. 138–147.
18. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. *Вісник НАН України*. 2014. 5. С. 65–69.
19. Zadiraka V., Kudin A., Shvidchenko I., Bredelev B. Cryptographic and steganographic protocols for cloud systems. *Computer technologies in information security*. Ternopil: "Kart-blansh", 2015. P. 9–41.
20. Zadiraka V., Yakymenko I., Kasianchuk M., Ivasyev S. Theoretical and numerical Krestenson's basis and its application to problems of cryptographic protection and factorization of multidigit numbers. *Computer technologies in information security*. Ternopil: "Kart-blansh", 2015. P. 216–260.
21. Zadiraka V., Smolarz A. Improving performance of two-key cryptography systems. *Computer technologies for information security*. Lublin: Politechnika Lubelska, 2011. P. 90–119.
22. Кудин А.М. Блокчейн и крипто валюті на основании «доказательства точності. *Математичне та компютерне моделювання*. Технічні науки. 2017. 15. С. 104–108. http://mcm-tech.kpnu.edu.ua/article/view/112002
23. Задирака В.К., Кудин А.М. Облачные вычисления в криптографии и стеганографии. *Кибернетика и системный анализ*. 2013. 4. С. 113–119.
24. Кудин А.М. Криптографические преобразования нешенноновских источников информации. *Кибернетика и системный анализ*. 2010. 5. С. 143–149
25. Vishnu M.B., Tiong S.K., Zaini M., Koh S.P. Security enhancement of digital motion image transmission using hybrid AES-DES algorithm. *Communications, APCC 2008. 14th Asian–Pacific Conference*. 2008. P. 1–5.
26. Parikh C., Patel P. Performance Evaluation of AES Algorithm on Various Development Platforms. *Consumer Electronics, ISCE* 2007. IEEE International Symposium. 2007. P. 1–6. https://doi.org/10.1109/ISCE.2007.4382134
27. Deshpande A., Deshpande M., Kayatanavar D.N. FPGA implementation of AES encryption and decryption. *2009 International Conference on Control, Automation, Communication and Energy Conservation*. Perundurai, India. 2009. P. 1–6.
28. Yenuguvanilanka J., Elkeelany O. Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. *IEEE SoutheastCon 2008*. Huntsville, AL, USA. 2008. P. 222–225. https://doi.org/10.1109/SECON.2008.4494289
29. Shao F., Chang Z., Zhang Y. AES Encryption Algorithm Based on the High Performance Computing of GPU. *2010 Second International Conference on Communication Software and Networks*. Singapore. 2010. P. 588–590. https://doi.org/10.1109/ICCSN.2010.124
30. Liu W., Luo R., Yang H. Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks. *2009 WRI International Conference on Communications and Mobile Computing*, Kunming, China. 2009. P. 496–501. https://doi.org/10.1109/CMC.2009.31
31. Lu C.-F., Kao Y.-S., Chiang H.-L., Yang Ch.-H. Fast implementation of AES cryptographic algorithms in smart cards. *IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology*. 2003. Proceedings. Taipei, Taiwan. 2003. P. 573–579, https://doi.org/10.1109/CCST.2003.1297622
32. Wadi S.M., Zainal N. High Definition Image Encryption Algorithm Based on AES Modification. *Wireless Pers Commun*. 2014. 79. P. 811–829. https://doi.org/10.1007/s11277-014-1888-7
33. Gaspar L., Drutarovsky M., Fischer V., Bochard N., Efficient AES S-boxes implementation for non-volatile FPGAs. *2009 International Conference on Field Programmable Logic and Applications*. Prague, Czech Republic. 2009. P. 649–653. https://doi.org/10.1109/FPL.2009.5272356
34. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems. *Advances in Cryptology-CRYPTO' 90. CRYPTO 1990*. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 1991. Vol 537. P. 2–11. https://doi.org/10.1007/3-540-38424-3_1

35. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag. 1993. 188 p. https://doi.org/10.1007/978-1-4613-9314-6
36. Matsui M. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology – EUROCRYPT '93. EUROCRYPT 1993*. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1994. Vol. 765. P. 386–397. https://doi.org/10.1007/3-540-48285-7_33
37. Михалевич В.С., Сергиенко И.В., Шор Н.З. Исследование алгоритмов решения оптимизационных задач и их приложения. *Кибернетика*. 1981. 4. С. 89–113.
38. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. 1996. 758 p.
39. Diffie W., Hellman M.E. New Directions in Cryptography. *IEEE Transactions on Information Theory*. 1976. **22** (6). P. 644–654. https://doi.org/10.1109/TIT.1976.1055608
40. Biham E. New Types of Cryptanalytic Attacks Using Related Keys. *Advances in Cryptology – EUROCRYPT '93. EUROCRYPT 1993*. Lecture Notes in Computer Science. 1994. Vol. 765. Springer, Berlin, Heidelberg. P. 398–409. https://doi.org/10.1007/3-540-48285-7_34
41. Matsui M. The First Experimental Cryptanalysis of the Data Encryption Standard. *In Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '94)*. 1994. Springer-Verlag, Berlin, Heidelberg. P. 1–11.
42. Nyberg K. Linear Approximation of Block Ciphers. *Advances in Cryptology – EUROCRYPT '94*. Ed. by Alfredo De Santis. Lecture Notes in Computer Science. Springer. 1995. 950. P. 439–444.
43. Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. *Advances in Cryptology — CRYPTO '96. CRYPTO 1996*. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 1996. Vol. 1109. P. 104–113. https://doi.org/10.1007/3-540-68697-5_9
44. Kocher P., Jaffe J., Jun B. Differential Power Analysis. *Advances in Cryptology — CRYPTO' 99. CRYPTO 1999*. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 1999. Vol. 1666. P. 388–397. https://doi.org/10.1007/3-540-48405-1_25
45. Brumley D., Boneh D. Remote timing attacks are practical. *Computer Networks 48*. 2005. 5. P. 701–716.
46. Xie Y., Zheng Y., Lian J. A Novel Image Parallel Chaotic Encryption Algorithm Based on Block Operation. *2023 3rd International Conference on Electronic Information Engineering and Computer Science (EIECS)*, Changchun, China. 2023. P. 384–388. https://doi.org/10.1109/EIECS59936.2023.10435566
47. Lesia M., Shchur G. Parallelization of Cryptographic Algorithm Based on Different Parallel Computing Technologies. *Symposium on Information Technologies & Applied Sciences*. 2021.

Одержано 25.10.2024

Баранов Ігор Анатолійович,
науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ.
https://orcid.org/0000-0002-5500-6210
vlasov@ukr.net

УДК 519.6

І.А. Баранов

Симетричний блочний алгоритм WBC1 та аналіз складності його реалізації

Інститут кібернетики імені В.М. Глушкова НАН України, Київ
Листування: vlasov@ukr.net

Вступ. Комп'ютерні мережі на сьогодні набувають все більшого значення для обміну інформацією. Криптографія відіграє життєво важливу роль у безпеці обчислень, зв'язку в мобільних телефонах, паролів у обчислювальній техніці та навіть інженерії, на відміну від давніх часів, коли криптографія полягала лише в шифруванні та розшифровці повідомлень за допомогою ключів. Одним з найважливіших вимог цих мереж є забезпечення безпечної передачі інформації з одного місця в інше. Криптографія є одним з методів, що забезпечують найбільш безпечний спосіб передачі конфіденційної інформації від відправника до передбачуваного отримувача.

В роботі описується симетричний блочний криптографічний алгоритм WBC1. Детально розглядається процес шифрування, аналіз складності алгоритму і швидкості виконання. Показана реалізація алгоритму.

Мета роботи – описати новий симетричний блочний криптографічний алгоритм WBC1, дослідити його складніть та швидкість виконання.

Результати. Побудовано блочний симетричний криптографічний алгоритм WBC1, досліджено аналіз складності та швидкість його виконання. На прикладах показано апробацію нового алгоритму.

Висновки. Алгоритм WBC1 представляє собою криптографічно стійкий метод шифрування, який забезпечує високий рівень безпеки за рахунок використання складних перестановок і циклічних зсувів. Для великих обсягів даних слід використовувати методи та алгоритми паралельних та розподілених обчислень для комп'ютерів з паралельною архітектурою. можливості представленого алгоритму досить великі. А можливість збільшення потужності алгоритму робить його гнучким для використання у різних областях та сферах діяльності, пов'язаних з обробкою інформації, що підлягає криптографічному захисту.

Ключові слова: симетричний блочний криптографічний алгоритм, криптографія, алгоритм.

UDC 519.6

Igor Baranov

Symmetric Block Algorithm WBC1 and Analysis of Its Implementation Complexity

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv
Correspondence: vlasov@ukr.net

Introduction. Nowadays, computer networks are gaining more and more importance for information exchange. Cryptography plays a vital role in the security of computing, mobile phone communication, passwords in computing and even engineering, unlike in the olden days when cryptography was only about encrypting and decrypting messages with keys. One of the most important requirements of these networks is to ensure the safe transfer of information from one place to another. Cryptography is one of the methods that provide the most secure way of transferring confidential information from the sender to the intended recipient.

The work describes the symmetric block cryptographic algorithm WBC1. The article examines the encryption process in detail, analyzes the complexity of the algorithm and the speed of execution. The implementation of the algorithm is shown.

The purpose of the work is to describe a new symmetric block cryptographic algorithm WBC1, to investigate its complexity and execution speed.

Results. The block symmetric cryptographic algorithm WBC1 was built, the complexity analysis and speed of its execution were studied. The examples show the approbation of the new algorithm.

Conclusions. The WBC1 algorithm is a cryptographically stable encryption method that provides a high level of security through the use of complex permutations and cyclic shifts. For large volumes of data, methods and algorithms of parallel and distributed calculations for computers with parallel architecture should be used. the capabilities of the presented algorithm are quite large. And the possibility of increasing the power of the algorithm makes it flexible for use in various areas and spheres of activity related to the processing of information subject to cryptographic protection.

Keywords: symmetric block cryptographic algorithm, cryptography, algorithm.