УДК 004.942:004.4:004.056.57 http://doi.org/10.15407/pp2022.03-04.417

ВДОСКОНАЛЕННЯ МЕТОДІВ ГЕНЕРАЦІЇ КЛЮЧІВ ШИФРУВАННЯ ЗА ДОПОМОГОЮ ДИВНИХ АТРАКТОРІВ

Володимир Шевченко, Ігор Сініцин, Віктор Шевченко

Актуальність роботи визначається потребою передачі конфіденційної інформації через відкриті канали комунікації. Така інформація може бути двох типів: симетричні ключі шифрування та безпосередньо інформаційні повідомлення, які зашифровані ключами шифрування. В статті розглянута задача вдосконалення передачі закритої інформації по відкритим каналам за допомогою алгоритму Диффі-Хелмана. Вдосконалення відбувається за рахунок введення нового типу односторонньої функції на основі чисельного рішення системи звичайних диференційних рівнянь, що описують динаміку руху фазової координати дивного атрактора. Для цього був розглянутий класичний алгоритм Диффі-Хелмана на основі односторонньої функції дискретного логарифму. Були розглянуті потрібні властивості односторонніх функцій у загальному випадку. Далі були розглянуті особливості модифікації алгоритму у випадку переходу до односторонньої функції на основі використання дивного атрактору. Передбачається, що на початку роботи модифікованого алгоритму таємним каналом сторони обміну (агенти) обмінюються інформацією щодо властивостей дивного атрактору, що буде використаний, а саме визначення диференційних рівнянь, що описують динаміку конкретного атрактору, значення параметрів рівнянь, початкові умови інтегрування та крок інтегрування (для методів з постійним кроком інтегрування). Відтак уесь обмін ведеться виключно відкритими каналами. В роботі також розглянутий випадок обміну інформацією між більш ніж двома агентами, зокрема, підхід щодо приховування кількості агентів, що беруть участь в обміні. Виконана апробація методу і наведені проміжні та кінцеві результати роботи односторонньої функції на основі дивних атракторів. Обговорені можливості щодо часткового викриття агентами окремих параметрів використання односторонніх функцій. Але водночас обгрунтована безпечність викриття такої інформації в загальному випадку (як в класичному, так й в модифікованому методі Діффі-Хелмана). Визначено, що залежно від потреб користувачів складність ключів шифрування може бути підвищена за допомогою зміни початкових параметрів атрактору, що також дозволить керувати швидкістю генерації ключів та шифрування загалом. Програмне забезпечення, що реалізує запропонований модифікований алгоритм, реалізовано трьома мовами програмування C#, Python та MatLab. Це дозволило виконати порівняльний аналіз результатів і свідомо обирати мову програмування окремих частин програмного забезпечення для оптимізації процесу генерації ключів шифрування для конкретних умов.

Ключові слова: захист інформації, обмін інформацією, алгоритм Диффі-Хелмана, односторонні функції, дивні атрактори, відкриті канали, ключі шифрування.

The urgency of the work is determined by the need to transfer confidential information through open communication channels. Such information can be of two types: symmetric encryption keys and directly informational messages that are encrypted with encryption keys. The article deals with the problem of improving the transmission of closed information over open channels using the Diffie-Hellman algorithm. The improvement is due to the introduction of a new type of one-sided function based on the numerical solution of the system of ordinary differential equations describing the dynamics of the phase coordinate movement of the strange attractor. For this purpose, the classic Diffie-Hellman algorithm based on the one-sided function of the discrete logarithm was considered. The required properties of one-sided functions in the general case were considered. Next, the peculiarities of algorithm modification in the case of transition to a one-sided function based on the use of a strange attractor were considered. It is assumed that at the beginning of the operation of the modified algorithm, through a secret channel, the exchange parties (agents) exchange information regarding the properties of the strange attractor to be used, namely, the definition of the differential equations describing the dynamics of a strange attractor, the values of the parameters of the equations, the initial integration conditions and the integration step (for methods with a constant step of integration). After that, all exchanges are conducted exclusively through open channels. The paper also considers the case of information exchange between more than two agents, in particular, the approach of hiding the number of agents participating in the exchange. Approbation of the method is carried out and intermediate and final results of the one-sided function based on strange attractors are given. Possibilities regarding partial disclosure by agents of certain parameters of the use of one-way functions are discussed. But at the same time, the safety of revealing such information is justified in the general case (both in the classical and in the modified Diffie-Hellman method). It was determined that depending on the needs of users, the complexity of the encryption keys can be increased by changing the initial parameters of the attractor, which will also allow controlling speed of key generation and encryption in general. The software that implements the proposed modified algorithm is implemented in three programming languages, C#, Python, and MatLab. This made it possible to perform a comparative analysis of the results and consciously choose the programming language of individual parts of the software to optimize the encryption key generation process for specific conditions.

Keywords: information protection, information exchange, Diffie-Hellman algorithm, one-way functions, strange attractors, open channels, encryption keys.

Вступ

У сучасних умовах обмін цифровою інформацією сягнув безпрецедентних масштабів і охопив усі сфери діяльності людства. Нормальна діяльність будь-якої країни та її громадян уже неможлива без інтенсивного обміну цифровою інформацією. Відповідно зростає актуальність захисту цієї інформації. Сьогодні недостатньо просто отримати корисну інформацію. В умовах постійних кібернетичних атак, які здебільшого носять епідеміологічний характер [1, 2], потрібно надійно захистити інформацію на всіх етапах її збору, обробки, зберігання, передачі. Захист інформації вимагає витрат досить великих ресурсів [3]. Одним із напрямків захисту інформації є шифрування [4]. Але злам шифрів сьогодні лише питання доступного машинного часу. В умовах постійного збільшення розрахункових можливостей комп'ютерів, а також зменшення

вартості їх використання, все складніше забезпечувати безпеку передачі та зберігання інформації в мережах Інтернет. Зазвичай паролі, що генеруються людьми, не є достатньо надійними, про це свідчать дослідження: досвідчений хакер за 4 години здатен зламати понад третину паролів, за тиждень – дві третини, за 5 тижнів 9 із 10 паролів.

Особливо гостро стоїть питання забезпечення безпечної передачі даних відкритими каналами зв'язку [5]. Нерідко інформацію необхідно передавати постійно та в великих обсягах, зокрема,передаючи дані між банками [6, 7, 8], або іншими великими компаніями. Для цього зазвичай використовується алгоритм Діффі-Хеллмана [9], що дозволяє створювати спільні ключі шифрування інформації. У його класичному варіанті для генерації ключів шифрування використовується **одностороння арифметична функція** з властивостями комутативності, наприклад, на основі дискретного логарифму [9]. Для дешифрування інформації зловмисник має знайти обернену функцію. В умовах, коли одностороння функція алгоритму хоча і є складною, але залишається арифметичною, підбір функції виглядає можливим та може бути виконаний за відносно невеликий проміжок часу (за наявності значних розрахункових потужностей, доступність яких що не день зростає). Тому збільшення зламостійкості шифрів шляхом пошуку принципово нових односторонніх функцій є актуальною задачею.

До прикладу, в роботах [8, 10] для створення односторонніх функцій були використані клітинні автомати з розширеним набором правил, щодо життя та вмирання клітин. Причиною такого вибору односторонньої функції було велике різноманіття варіантів поведінки колоній клітинних автоматів. Це забезпечувало, з одного боку, квазівипадковість поведінки моделі а, з іншого – абсолютну повторюваність результатів моделювання. Аналогічний ефект могло би дати моделювання динаміки об'єктів екосистем реального світу на основі систем звичайних диференційних рівнянь [11] або моделі детермінованого хаосу [12. Але чисельні розв'язки звичайних диференційих рівнянь досить передбачувані, а моделі детермінованого хаосу потребують більшої різноманітності. У якості рішення в даній роботі запропоновано використовувати моделі дивних атракторів.

Розглянемо можливості створення односторонніх функцій на основі чисельного розв'язку диференційних рівнянь, що описують динаміку поведінки дивних атракторів. Наразі відомо багато дивних атракторів. Усі вони мають хаотичний характер, що робить можливим їх використання для генерації псевдовипадкових чисел. Водночас вони також мають достатньо високий рівень відтворюваності при чисельному розрахунку їх фазових траєкторій.

Мета роботи. Покращити якість процесу створення спільних ключів шифрування за допомогою відкритих каналів зв'язку в рамках алгоритму Діффі-Хеллмана за допомогою створення односторонньої функції на основі модифікованих дивних атракторів.

1. Класичний алгоритм Діффі-Хеллмана

Розглянемо класичний варіант алгоритму Діффі-Хеллмана.

В умовах, коли необхідно постійно змінювати паролі або ключі шифрування доступ до закритих каналів зв'язку зазвичай або відсутній, або потребує занадто багато ресурсів. Алгоритм Діффі-Хеллмана дозволяє для генерації ключів шифрування використовувати відкриті канали зв'язку без відчутного ризику компрометації згенерованих ключів. Точніше, агенти мають лише одну можливість скористатися закритим каналом зв'язку, але все наступне спілкування відбувається відкритими каналами зв'язку.

Алгоритм виглядає таким чином:

1. При першому зв'язку закритим каналом агенти визначають властивості односторонньої функції. У класичному варіанті алгоритму за односторонню функцію використовують дискретний логарифм [9, 13]. В нашому випадку пропонується використовувати дивний атрактор, для якого в цьому сеансі зв'язку визначаються всі необхідні властивості: диференційні рівняння, що описують динаміку конкретного атрактору, значення параметрів рівнянь, початкові умови інтегрування та крок інтегрування (для методів з постійним кроком інтегрування).

2. Перший агент формує таємне слово $x1$ (в нашому випадку кількість кроків інтегрування атрактора). При цьому параметр $y0$ є початковим значенням функції (в нашому випадку початкові координати точки в просторі, з якої починається побудова атрактора). Перший агент знаходить проміжне значення функції

$$y1 = f(y0, x1)$$

і через відкритий канал надсилає проміжне значення функції другому агенту.

3. Другий агент отримує проміжне значення функції $y1$ від першого агенту, формує своє таємне слово $x2$ та використовує ту ж саму функцію. Тепер другий агент знає новий ключ шифрування

$$y12 = f(y1, x2).$$

4. Далі агенти діють аналогічно (пп.2, 3), але тепер вони міняються місцями:

$$y2 = f(y0, x2); \quad y21 = f(y2, x1).$$

Оскільки функція комутативна, то

$$y21 = f(y2, x1) = f(y1, x2) = y12.$$

Отже, обидва агенти сформували у себе новий ключ шифрування $y21$.

Імовірні зловмисники прослуховують відкритий канал, знають проміжні значення функції $y1, y2$, але при цьому не знають нового ключа $y21$ та початкових значень $y0$.

2. Класичні односторонні функції

Як вже було сказано, одним із поширених варіантів односторонньої функції є дискретний логарифм. Розглянемо її використання для розглянутого вище алгоритму Діффі-Хеллмана.

На початку агенти формують деякі числа g і p, які не є таємними і можливо відомі зловмиснику. Після цього агент 1 та агент 2 окремо формують таємні слова - дуже великі числа $x1$, $x2$ та кожен використовує їх для формування проміжних значень односторонніїї функції.

$$y1 = g^{x1} mod\ p$$

$$y2 = g^{x2} mod\ p$$

$y1$ та $y2$ агенти надсилають відкритим каналом один одному і повторюють ту ж процедуру з тим, що отримали від колеги

$$y1^{x2} = g^{x1x2} mod\ p = y3,$$

$$y2^{x1} = g^{x2x1} mod\ p = y3.$$

Як і в розглянутому вище узагальненому алгоритмі обидва агенти відкритим каналом отримали інформацію, яка дозволила їм сформувати спільний таємний код $y3$. Постановка задачі знаходження зворотного дискретного логарифму проглядається досить чітко. Тому криптоаналітики намагаються викрити ключ за рахунок збільшення обчислювальних потужностей. Якщо ж використовувати якісь незвичні односторонні функції, то для криптоаналітика задача може суттєво ускладнитись. Відповідно зламостійкість методу також суттєво збільшиться.

3. Постановка задачі

Загальні умови

1. Потрібно створити метод, який дозволяє генерувати ключі шифрування, як завгодно часто, за допомогою лише відкритого каналу обміну інформацією.

2. На початку роботи алгоритму відбувається хоча б один таємний обмін інформацією щодо виду, властивостей, параметрів односторонньої функції та алгоритму взаємодії агентів у визначенні нового ключа шифрування.

3. Кількість агентів може бути довільною з урахуванням потрібної загальної кількості адрес взаємного обміну таємними повідомленнями.

4. Базовим доцільного взяти алгоритм Діффі-Хеллмана та модифікувати його.

Визначення процедури роботи односторонньої функції на основі дивних атракторів.

По-перше, декомпозуємо задачу на 2 складові:

1. Розробити способи перетворення результату роботи дивного атрактора на те, що може бути сприйняте, як результат роботи односторонньої функції.

2. Модифікувати властивості дивних атракторів за рахунок вибору початкових умов, параметрів диференційних рівнянь та, в окремих випадках, вибором величини кроку інтегрування, для урізноманітнення варіантів поведінки функції.

Властивості функції:

- Односторонність. Тобто можливість отримання значення функції на основі інформації про аргумент $y = f(x)$

і одночасна неможливість отримання значення аргументу на основі значення функції, точніше кажучи відсутність зворотної функції, яка б забезпечила знаходження аргументу для заданого значення функції $x = f^{-1}(y)$.

У випадку з дивними атракторами властивість односторонності не може бути отримана без введення додаткових модифікацій, оскільки будь-який атрактор, який можна представити у вигляді системи диференційних рівнянь (в даній роботі розглядаються саме такі атрактори), що робить можливим знаходження $x = f^{-1}(y)$ на основі відомих характеристик атрактора. Для того, щоб дивний атрактор набув властивості односторонності пропонується на кожному кроці інтегрування за методом Ейлера округлювати отримані числа до певного порядку. Наприклад:

На ітерації t_n було отримано значення координат точки A_n – (0.641, -1.345, 123.532). В такому випадку перед розрахунком координат наступної точки A_{n+1} необхідно округлити значення точки A_n до першого знаку після коми, в результаті отримаємо: $A_n{}'$ – (0.6, -1.4, 123.5), що і буде використано для обрахунку наступної точки A_{n+1}.

Хоча зміни значень координат точки суто чисельно можна вважати незначними, однак у разі накопиченння «похибки» значення для чергової точки можуть відрізнятися від тих, що могли бути без «похибки». Саме ця модифікація надає атрактору властивості односторонності, оскільки під час формування ключів шифрування агентам ніщо не заважає у проведені операцій. Якщо ж зловмисних спробує знайти обернену функцію, йому це не вдасться, оскільки будуть невідомі ті округлення, що робилися під час обрахунків.

- Комутативність. Якщо позначити дію функції знаком «×», то властивість комутативності групових операцій ознає $x1 \times x2 = x2 \times x1$.

На прикладі функції це може бути

$$f(x1 \times x2) = f(x2 \times x1),$$
$$f(x1 + x2) = f(x2 + x1).$$
$$f(x1, x2) = f(x2, x1)$$

4. Модифікація алгоритму Діффі-Хеллмана для n агентів

Нехай потрібно згенерувати єдиний пароль для n агентів. Алгоритм у такому випадку виглядатиме аналогічно, за винятком деяких особливостей:

1. В перший сеанс зв'язку таємним каналом агенти так само, як у випадку двох агентів, домовляються про параметри функції перетворення $f(x)$ та супутні дані. Усе інше спілкування відбувається через відкриті канали зв'язку.

2. У разі потреби зміни ключа шифрування, всі агенти i формують таємні слова $xi, \quad i = \overline{1,n}$ та розраховують проміжні значення функції першого рівня

$$yi^{(1)} = f(y0, xi), \quad i = \overline{1,n}.$$

Значення $yi^{(1)}$ кожен агент i відкритим каналом циклічно надсилає агенту $i + 1$. Циклічність означає, що агент n надсилає проміжні значення 1 рівня агенту 1. Якщо сказати узагальнено, то номер наступного агента дорівнює залишку від ділення $i + 1$ за модулем n.

$$r = (i + 1) \ mod \ n.$$

3. Тепер кожен агент r на кожному новому кроці k опрацьовує інформацію від попередніх агентів $yi^{(k-1)}$. Для цього він щоразу використовує своє таємне слово xr. Тільки проміжне значення функції $yi^{(k-1)}$ кожного разу змінюється. Нове проміжне значення дорівнює

$$yr^{(k)} = f\left(yi^{(k-1)}, xr\right), \quad i = \overline{1,n}.$$

4. На кроці n кожен агент отримає проміжне значення функції, яке він за допомогою свого таємного слова перетворить на новий спільний ключ шифрування.

$$yr^{(n)} = f\left(yi^{(n-1)}, xr\right), \quad i = \overline{1,n}.$$

Під час генерації ключів шифрування агенти співпрацюють лише з двома агентами: з відправником проміжного значення функції та агентом-приймачем. Інформація про інших агентів недоступна.

Ймовірні зловмисники, як і в двоагентному випадку, прослуховують відкритий канал, знають проміжні значення функції від всіх агентів, але не знають ані нового ключа шифрування, ані таємних слів від окремих агентів.

Заплутування інформації щодо кількості агентів

Для збереження в таємниці інформації щодо кількості агентів, в роботі пропонується, щоб один з агентів «грав» замість декількох агентів. Це створить враження, що агентів більше, ніж їх є насправді. Але водночас фальшивих агентів не має бути занадто багато, оскільки в такому разі зловмисник отримує більше інформації про проміжні значення функції, за допомогою чого може легше підібрати параметри атрактору та параметри чисельного інтегрування.

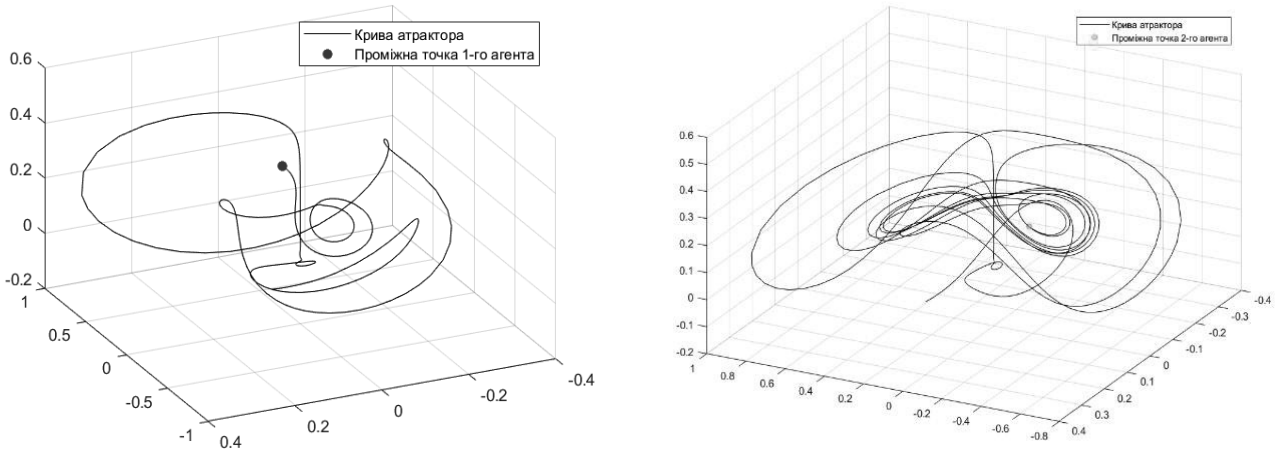
5. Апробація модифікованого алгоритму Діффі-Хеллмана

За односторонню функцію, зокрема, був використаний атрактор Ньютона-Лейпніка. Загалом як одностороння функція може бути використаний будь-який атрактор за умови, що початкові параметри атрактора, які були сформовані під час першого контакту, зберігаються в таємниці.

На основі випадкового графічного зображення (рис. 1) агенти формують однаковий набір параметрів та початкових значень для рішення системи диференціальних рівнянь дивних атракторів.

Рис. 1. Зображення для генерації початкових координат атрактора.

Відтак кожен з агентів придумав своє таємне слово (наприклад, 50 у першого і 100 у другого), яке відповідає кількості ітерацій інтегрування атрактора, знаходить проміжні координати атрактора та відправляє їх іншому агенту. Після чого отримані проміжні координати (рис. 2 а, б) мають бути використані для проходження відомої кількості ітерацій інтегрування (50 у першого і 100 у другого відповідно). У першого агента це 100+50=150 кроків. У другого 50+100=150 кроків. Отже обидва агенти різними шляхами отримують однакові кінцеві координати (рис. 3). Криву атрактора з проміжними та кінцевою точкою разом зображено на рис. 4. Критично оцінюючи односторонні функції як класичного дискретного логарифму, так і чисельного інтегрування дивного атрактору слід відзначити, що насправді обидва агенти можуть шляхом моделювання вирахувати, яку саме кількість кроків як таємне слово використав інший агент. Для цього достатньо просто промоделювати динаміку атрактора не повну кількість кроків (в нашому випадку 150) і на кожному кроці порівняти результат з проміжними координатами атрактора від іншого агента. Але це додатково нічого не дає, оскільки наступного разу будуть використані інші величини кроків. Цього ж разу кінцевий результат (на 150 кроці) і так відомий обом агентам, які належать до певної групи довіри.



а) б)

Рис. 2. Ітерації атрактора з виділеними проміжними точками.
а) з проміжною точкою агенту 1; б) проміжною точкою агенту 2.

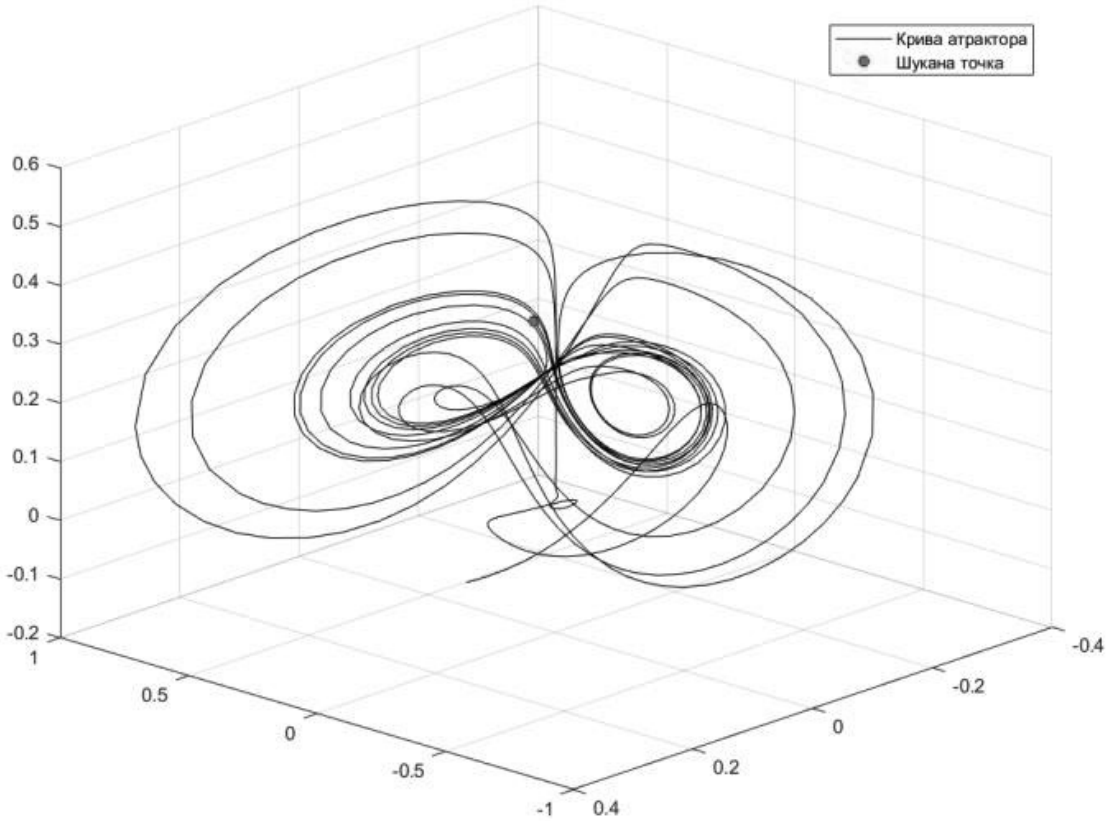


Рис. 3. Ітерації атрактора з виділеною проміжною точкою.

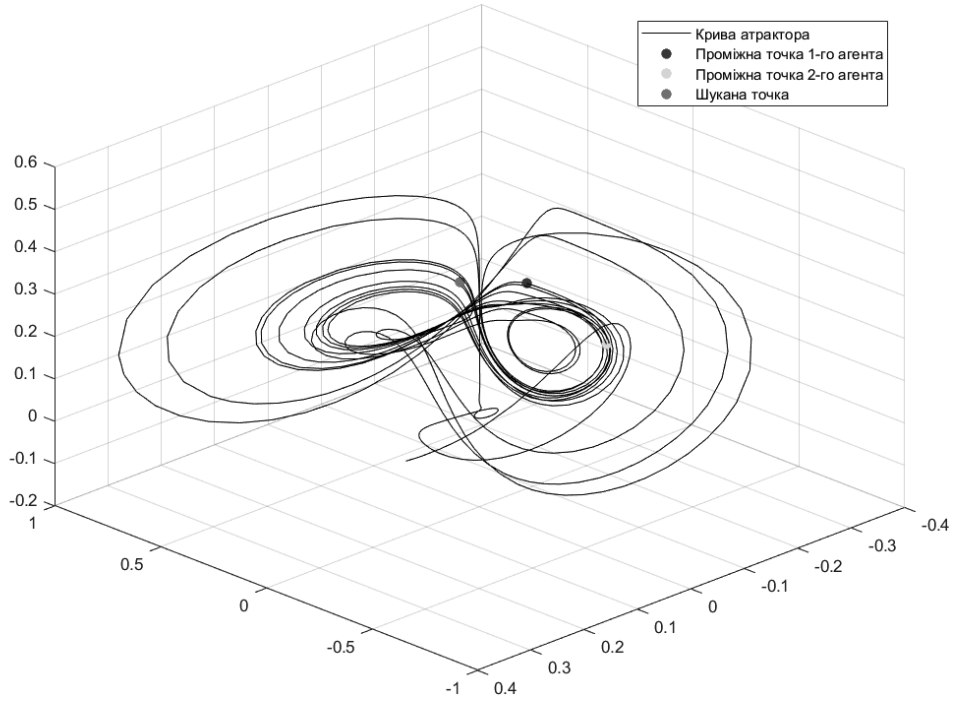


Рис. 4. Графік із зображенням проміжних та кінцевої точки на кривій атрактора.

Далі отримані кінцеві координати можуть використовуватись залежно від встановлених вимог до захисту: безпосередньо у двійковому вигляді, безпосередньо у шістнадцятирічному, або у вигляді хеша (рис. 5).

3226332823302120272716282118292323192823292220282223193025232618272
4153014232225282522172221262628263124242824272121262223202425213020
3322272922293822351934352821333926302726131724201730242524303525 32

Рис. 5. Спільний ключ шифрування на основі кінцевих координат.

Висновки

1. На основі отриманих наукових та прикладних результатів можна стверджувати, що мета роботи «покращити якість процесу створення спільних ключів шифрування за допомогою відкритих каналів зв'язку в рамках алгоритму Діффі-Хеллмана за допомогою створення односторонньої функції на основі дивних атракторів» досягнута.

2. У роботі вдосконалено алгоритм Діффі-Хеллмана,с використавши створення односторонньої функції на базі дивних атракторів.

3. Створений алгоритм із модифікованою односторонньою функцією на базі дивного атрактора може бути використаний для створення ключів шифрування та паролів для безпечної передачі інформації.

4. Залежно від потреб користувачів складність ключів шифрування може бути підвищена за допомогою зміни початкових параметрів атрактору, що також дозволить керувати швидкістю генерації ключів та шифрування загалом.

5. Програмне забезпечення реалізовано трьома мовами програмування C#, Python та MatLab, що дозволяє здійснювати порівняльний аналіз результатів і свідомо обирати мову програмування окремих частин програмного забезпечення для оптимізації процесу генерації ключів шифрування.

6. Подальший напрям досліджень доцільно спрямувати в бік систематизації моделей дивних атракторів з визначенням особливостей, що впливають на зламостійкість алгоритму Діффі-Хелмана.

Література

1. Shevchenko V.L., Nesterenko O.V., Netesin I.E., Shevchenko A.V., Polishchuk V.B. Prognostic modeling of computer virus epidemics. - K.: UkrSC IND, 2019. - 152 p.
2. Viktor Shevchenko, Alina Shevchenko. The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems. - 2017 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Polyana, April 20-23, 2017. - p.174-177. doi.org/10.1109/MEMSTECH.2017.7937561.
3. Shevchenko Viktor, Alina Shevchenko, Ruslan Fedorenko, Yurii Shmorhun, Asadi Hrebennikov. Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses. - CADSM 2019, 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), February 26 – March 2, 2019, Polyana-Svalyava (Zakarpattya), UKRAINE, IEEE Ukraine Section, IEEE Ukraine Section (West), MTT/ED/AP/EP/SSC Societies Joint Chapter Part Number: CFP19508-USB ISBN: 978-1-7281-0053-1 pp.36-40.

4. Mitsuru Matsui Robert - Selected Areas in Cryptography / Zuccherato Henri Gilbert, Helena Handschuh // Security Analysis of SHA-256 and Sisters – August 14 – August 15, 2003, Ottawa, Canada, pp. 175 – 193. doi.org/10.1007/978-3-540-24654-1_13
5. Philip MacKenzie, Thomas Shrimpton, Markus Jakobsson. Threshold Password-Authenticated Key Exchange. // Journal of Cryptology, Vol. 19, Issue 1, January 2006, pp. 27-66. doi.org/10.1007/s00145-005-0232-5
6. Petrov, P., Dimitrov, G., Ivanov, S. "A Comparative Study on WebSecurity Technologies UsedinIrish and FinnishBanks." 18 International Multidisciplinary ScientificGeoconference SGEM 2018: Conference Proceedings, 2 - 8 July 2018, Albena, Bulgaria : Vol. 18. Informatics, Geoinformatics a. RemoteSensing. Iss. 2.1. Informatics, Sofia : STEF92 Technology Ltd., Vol. 18, 2018, Iss. 2.1, pp. 3 - 10.
7. Pavel Petrov, Stefan Krumovich, Nikola Nikolov, Georgi Dimitrov, and Vladimir Sulov. 2018. "Web Technologies Used in the Commercial Banks in Finland." InProceedingsofthe 19th International Conference on Computer Systems and Technologies (CompSysTech'18), Boris Rachev and Angel Smrikarov (Eds.). ACM, New York, NY, USA, pp. 94-98. DOI: https://doi.org/10.1145/3274005.3274018. ISBN: 978-1-4503-6425-6
8. Volodymyr Shevchenko; Georgi Dimitrov; Denys Berestov; Pepa Petrova; Igor Sinitcyn; Eugenia Kovatcheva; Ivan Garvanov; Iva Kostadinova One-way Function Based on Modified Cellular Automata in the Diffie-Hellman Algorithm for Big Data Exchange Tasks through Open Space. – DIGILIENCE 2020: Cyber Protection of Critical Infrastructures, Big Data and Artificial Intelligence. – Varna, September 30 – October 2, 2020. – pp.233-246. http://isij.eu/isij-47-digilience-2020-cyber-protection-critical-infrastructures-big-data-and-artificial
9. Whitfield Diffie and Martin E. Hellman. IEEE Transaction on Information Theory. Vol. IT-22, No.6, November 1976, pp.644-654.
10. Volodymyr Shevchenko, Denis Berestov, Igor Sinitcyn, Viktor Shevchenko Built-In Processor for Sharing Passwords Through the Open Information Space. - 2020 16-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Lviv, April 22-26, 2020. - pp.40-44. doi.org/10.1109/MEMSTECH49584.2020.9109523
11. Aleksandr Lysenko, Aleksej Bychkov, Sergey Chumachenko, Galina Panajotova, Evgenija Kovacheva, Viktor Shevchenko, Andrej Turejchuk. Mathematical models and information technology for assessing and predicting environmental conditions at landfills. Publisher: Pro Langs, Kyiv-Sofia 2017, ISBN: 978-954-2995-29-6 pp.1-218.
12. Shevchenko V.L. Optimization Modeling in Strategic Planning. - K.: CVSD NUOU, 2011. – 283p.
13. Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301. DOI: 10.4018/978-1-5225-2773-2.

References

1. Shevchenko V.L., Nesterenko O.V., Netesin I.E., Shevchenko A.V., Polishchuk V.B. Prognostic modeling of computer virus epidemics. - K.: UkrSC IND, 2019. - 152 p.
2. Viktor Shevchenko, Alina Shevchenko. The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems. - 2017 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Polyana, April 20-23, 2017. - p.174-177. doi.org/10.1109/MEMSTECH.2017.7937561.
3. Shevchenko Viktor, Alina Shevchenko, Ruslan Fedorenko, Yurii Shmorhun, Asadi Hrebennikov. Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses. - CADSM 2019, 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), February 26 – March 2, 2019, Polyana-Svalyava (Zakarpattya), UKRAINE, IEEE Ukraine Section, IEEE Ukraine Section (West), MTT/ED/AP/EP/SSC Societies Joint Chapter Part Number: CFP19508-USB ISBN: 978-1-7281-0053-1 pp.36-40.
4. Mitsuru Matsui Robert - Selected Areas in Cryptography / Zuccherato Henri Gilbert, Helena Handschuh // Security Analysis of SHA-256 and Sisters – August 14 – August 15, 2003, Ottawa, Canada, pp. 175 – 193. doi.org/10.1007/978-3-540-24654-1_13
5. Philip MacKenzie, Thomas Shrimpton, Markus Jakobsson. Threshold Password-Authenticated Key Exchange. // Journal of Cryptology, Vol. 19, Issue 1, January 2006, pp. 27-66. doi.org/10.1007/s00145-005-0232-5
6. Petrov, P., Dimitrov, G., Ivanov, S. "A Comparative Study on WebSecurity Technologies UsedinIrish and FinnishBanks." 18 International Multidisc iplinaryScientificGeoconference SGEM 2018: Conference Proceedings, 2 - 8 July 2018, Albena, Bulgaria : Vol. 18. Informatics, Geoinformatics a. RemoteSensing. Iss. 2.1. Informatics, Sofia : STEF92 Technology Ltd., Vol. 18, 2018, Iss. 2.1, pp. 3 - 10.
7. Pavel Petrov, Stefan Krumovich, Nikola Nikolov, Georgi Dimitrov, and Vladimir Sulov. 2018. "Web Technologies Used in the Commercial Banks in Finland." InProceedingsofthe 19th International Conference on Computer Systems and Technologies (CompSysTech'18), Boris Rachev and Angel Smrikarov (Eds.). ACM, New York, NY, USA, pp. 94-98. DOI: https://doi.org/10.1145/3274005.3274018. ISBN: 978-1-4503-6425-6
8. Volodymyr Shevchenko; Georgi Dimitrov; Denys Berestov; Pepa Petrova; Igor Sinitcyn; Eugenia Kovatcheva; Ivan Garvanov; Iva Kostadinova One-way Function Based on Modified Cellular Automata in the Diffie-Hellman Algorithm for Big Data Exchange Tasks through Open Space. – DIGILIENCE 2020: Cyber Protection of Critical Infrastructures, Big Data and Artificial Intelligence. – Varna, September 30 – October 2, 2020. – pp.233-246. http://isij.eu/isij-47-digilience-2020-cyber-protection-critical-infrastructures-big-data-and-artificial
9. Whitfield Diffie and Martin E. Hellman. IEEE Transaction on Information Theory. Vol. IT-22, No.6, November 1976, pp.644-654.
10. Volodymyr Shevchenko, Denis Berestov, Igor Sinitcyn, Viktor Shevchenko Built-In Processor for Sharing Passwords Through the Open Information Space. - 2020 16-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Lviv, April 22-26, 2020. - pp.40-44. doi.org/10.1109/MEMSTECH49584.2020.9109523
11. Aleksandr Lysenko, Aleksej Bychkov, Sergey Chumachenko, Galina Panajotova, Evgenija Kovacheva, Viktor Shevchenko, Andrej Turejchuk. Mathematical models and information technology for assessing and predicting environmental conditions at landfills. Publisher: Pro Langs, Kyiv-Sofia 2017, ISBN: 978-954-2995-29-6 pp.1-218.
12. Shevchenko V.L. Optimization Modeling in Strategic Planning. - K.: CVSD NUOU, 2011. – 283p.
13. Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301. DOI: 10.4018/978-1-5225-2773-2.

Одержано 02.09.2022

Про авторів:

Шевченко Володимир Вікторович,
студент бакалаврату.
Кількість публікацій в українських виданнях – понад 10.
Кількість зарубіжних публікацій – 3.
Індекс Хірша – 1.
https://orcid.org/0000-0002-2152-6816.

Сініцин Ігор Петрович,
доктор технічних наук,
старший науковий співробітник.
Кількість публікацій в українських виданнях – понад 80.
Індекс Хірша – 1.
https://orcid.org/0000-0002-4120-0784.

Шевченко Віктор Леонідович,
доктор технічних наук,
професор.
Кількість публікацій в українських виданнях – понад 300.
Кількість зарубіжних публікацій – 17.
Індекс Хірша – 4.
https://orcid.org/0000-0002-9457-7454.

Місце роботи авторів:

Інститут програмних систем НАН України, 03187, м. Київ-187,
проспект Академіка Глушкова, 40.
Тел.: (38)(044) 526-21-48
E-mail: ukrprog@isofts.kiev.ua

Київський національний університет імені Тараса Шевченка
Вул. Богдана Гаврилишина, 24, Київ, Україна, 02000.
Тел.: (38)(097) 016-69-21
E-mail: vladimir_337@ukr.net

Прізвища та ім’я авторів і назва доповіді українською мовою:
Шевченко В.В., Сініцин І.П., Шевченко В.Л.
Вдосконалення методів генерації ключів шифрування
за допомогою дивних атракторів

Прізвища та ім’я авторів і назва доповіді англійською мовою:
ShevchenkoV.V., Sinitsyn I.P., Shevchenko V.L.
Improving methods for generating encryption keys using strange attractors