DOI 10.31891/2307-5732-2020-291-6-33-38
УДК 004.891

В.М. ДЖУЛІЙ, І.В. МУЛЯР, В.С. ОРЛЕНКО, В.Ю. ТІТОВА, В.А. АНІКІН
Хмельницький національний університет

СИМЕТРИЧНА КРИПТОСИСТЕМА З НЕЛІНІЙНИМ ШИФРУВАННЯМ ТА МОЖЛИВІСТЮ КОНТРОЛЮ ШИФРОТЕКСТУ З МЕТОЮ МАСКУВАННЯ

В статті запропонована проста симетрична перестановочна криптосистема, перестановки в якій відбуваються на основі потокової генерації випадкових чисел. Наведений криптографічний алгоритм, в зв'язку з нелінійністю процесу шифрування, здатний шифрувати одні і ті ж блоки інформації по-різному. Дана властивість може бути використана для формування шифротексту конкретного вигляду та, як наслідок, для прихованої передачі шифрованих повідомлень і повного, або часткового маскування факту криптографічного впливу.

Підстановочно-перестановочні алгоритми достатньо розповсюджені на сьогоднішній день. Вони зарекомендували себе як надійні криптостійкі шифри, що склали серйозну конкуренцію ітеративним математичним шифрам, на базі мережі Фейстеля, та поступово все більше та більше витісняють їх, займаючи їх місце.

В статті запропонований алгоритм шифрування, який має просту структуру та легкий в реалізації, але при цьому, прогнозовано, він є достатньо стійким для криптоатак, має високу швидкість роботи та використовує всі переваги сучасних алгоритмів шифрування та має потенціал для маскування шифрованих даних.

Розроблено схему шифрування, в якій перестановки відбуваються у випадковому порядку, та, як наслідок, стає можливою ситуація, коли одному відкритому тексту при одному і тому ж ключі відповідає безліч шифротекстів, що серйозно ускладнює роботу криптоаналітиків, ускладнюючи аналіз та злом шифру, а також суттєво збільшує область прикладного використання даної криптосистеми. Також дана криптосистема має стеганографічний потенціал, оскільки нелінійність, яка породжує варіативність шифротекстів, дозволяє, фактично, один і той ж самий байт зашифрувати десятками, або навіть сотнями комбінацій.

Запропоновано новий підхід до створення шифрувальної варіативності та випадкового вибору, що дає можливість модифікації вже існуючих алгоритмів шифрування.

Ключові слова: криптографія, стеганографія, симетрична криптосистема, перестановочний шифр, випадкова генерація, захист інформації.

V. DZHULIY, I. MULYAR, V. ORLENKO, V. TITOVA, V. ANIKIN
Khmelnytsky National University, Khmelnytsky, Ukraine

SYMMETRIC CRYPTOSYSTEM WITH NONLINEAR ENCRYPTION AND THE POSSIBILITY OF CONTROL OF CIPHERTEXT FOR CONCEALMENT

The article proposes a simple symmetric permutation cryptosystem, in which permutations occur based on streaming generation of random numbers.

Substitution-permutation algorithms are quite common today. They have proven to be reliable crypto-strong ciphers that have seriously competed with iterative mathematical ciphers, based on the Feistel network, and are gradually displacing them more and more, taking their place.

The aim of the article is to propose an encryption algorithm that has a simple structure and is easy to implement. At the same time, it is estimated to be quite resistant to crypto attacks. This encryption algorithm has a high speed and uses all the advantages of permutation encryption algorithms.

Developed an encryption scheme in which permutations occur randomly, and as a result, a situation becomes possible when one plaintext with the same key corresponds to many ciphertexts, which seriously complicates the work of cryptanalysts, complicating the analysis and cracking of the cipher, and significantly increases the scope of application of this cryptosystem. Also, this cryptosystem has steganographic potential, because the nonlinearity that creates the variability of ciphertexts, allows the same byte to encrypt dozens or even hundreds of combinations.

This paper has clearly shown a new approach to the creation of encryption variability and random selection is proposed. It makes possible to modify existing encryption algorithms.

Key words: cryptography, steganography, symmetric cryptosystem, permutation cipher, random generation, information protection.

Вступ

У всі часи люди намагалися захищати інформацію, яку вважають важливою, постійно розвиваючи та удосконалюючи засоби для її захисту. Стислий Оксфордський словник англійської мови визначає криптографію як «мистецтво написання або розв'язування кодів". Це історично точно, але воно не враховує сучасної розповсюдженості галузі та її сьогоденних наукових основ [1]. На сьогоднішній день криптографія має вкрай широкий спектр застосувань, починаючи від класичного захисту інформації при зберіганні, чи передачі, закінчуючи контролем цілісності повідомлень та цифровими підписами, для верифікації даних.

Також здавна люди намагались приховувати ту чи іншу інформацію, різноманітними способами маскуючи її. Такі починання згодом переросли в науку під назвою стеганографія, що на сьогоднішній день широко використовується в сфері захисту інформації.

У розрізі цього, не видається дивним що здавна і до сьогодні люди працюють над розробкою нових і нових криптосистем: шифр Цезаря змінили криптосистеми простої заміни, їх, в свою чергу, витіснили поліалфавітні системи, на кшталт шифрів Гронсфельда та Віженера [2], а їх, пізніше, – ітеративні блочні шифри, на основі мережі Фейстеля, яскравим прикладом яких є DES [3], різноманітні модифікації якого широко використовуються до сьогоднішнього дня.

Разом із розвитком криптосистем, невпинно розвивався і криптоаналіз, накопичений інструментарій якого [4], у поєднанні з технічними можливостями сучасної обчислювальної техніки, задає вкрай високу планку вимог для сучасної криптографії вцілому та безпосередньо для використовуваних криптосистем.

На сьогоднішній день одними з найбільш захищених криптосистем у світі є шифри, на основі підстановочно–перестановочних систем, наприклад SQUARE та Rijndael, останній відомий на широкий загал як Advanced Encryption Standard (AES) [3, 5].

З огляду на це, можна стверджувати що підстановочно–перестановочні системи, спроектовані таким чином, щоб максимально використовувати сучасні обчислювальні потужності та досягати високої ентропії при шифруванні, здатні надійно захищати інформацію та є стійкими до сучасних криптоатак.

Також, безумовно, важливою складовою захисту інформації є непомітність. Логічно, що інформацію, яка виглядає цілісно, осмислено, без слідів того що в ній щось приховано, або зашифровано, навряд чи хто буде досліджувати без суттєвих на те підстав. Саме через це в сучасному світі, у сфері кібербезпеки, все частіше використовується стеганографія – наука, що до надає інструментарій для приховування однієї, умовно «таємної», інформації всередині іншої – публічної, тієї що не представляє для сторонніх осіб жодного інтересу. В зв'язку з цим, виникає великий попит на алгоритми, які підходять до захисту комплексно: вони здатні як захистити інформацію криптографічно, так і, повністю, або частково, замаскувати сам факт того що деяка інформація була прихована.

Огляд літературних джерел

Симетричні криптосистеми давно відомі науці та є в достатній мірі вивчені та проаналізовані. В зв'язку з цим, дослідження симетричних систем шифрування знайшло відбиток у великій кількості наукових статей та літературі. Дані напрацювання обов'язково слід враховувати при розробці криптосистеми.

Симетричні криптосистеми на протязі багатьох століть використовувались для захисту інформації та «закриття» важливої інформації від несанкціонованого використання [6, 7, 8]

Симетричні алгоритми шифрування перетворюють деяку конфіденційну інформацію, на основі криптографічного ключа, у шифровану форму. Зворотне перетворення, яке відновлює вхідну інформацію, відбувається при зворотному виконанні алгоритму, за умови, що у вас є такий цей ж самий ключ [8]. Сучасні симетричні криптосистеми, хоч і є більш витонченими, математично та комбінаторно обґрунтованими, все одно, як правило дотримуються таких принципів.

Також важливою складовою при розробці криптосистеми є оцінка інструментарію криптоаналізу, та сучасні можливості у сфері «взлому» систем шифрування. Для створення криптостійкого алгоритму слід на етапі проектування враховувати те, яким чином він буде поводитись під час криптоатаки та забезпечити достатній запас міцності та стійкості [9 - 11].

Постановка задачі

Необхідно створити простий у реалізації криптостійкий перестановочний симетричний алгоритм шифрування, який би відповідав сучасним вимогам безпеки та значно ускладнював існуючі способи криптоаналізу, при цьому з можливістю корегування вихідного шифротексту.

Основна ідея даного алгоритму полягає в тому, що Р-блок, за яким відбуватиметься перестановка, для кожного байту обирається випадково, на основі генератора випадкових чисел. Такий підхід значно ускладнить будь-який статистичний криптоаналіз, оскільки будь-які закономірності між відкритими байтами та зашифрованими будуть відсутні. Потокова випадкова генерація коефіцієнта перестановки дозволить досягти неоднорідності шифрування та відсутності закономірностей у ньому.

Також, через відсутність складної ітеративності, даний алгоритм повинен мати високу швидкість роботи, порівняно з аналогами.

Основна частина

Відповідно до поставленої задачі, криптосистема повинна відповідати сучасним вимогам безпеки, бути надійною та придатною для практичного використання, забезпечуючи високу надійність, а отже, даний шифр повинен бути стійким перед інструментарем сучасного криптоаналізу.

Одною з головних потужностей криптоаналізу на сьогодні є обчислювальна потужність комп'ютерної техніки, яка серйозно збільшується з кожним новим поколінням. Фактично будь-який симетричний шифр можливо взламати атакою «грубої сили», тобто повним перебором всіх можливих криптографічних ключів, та почерговими спробами розшифрування кожним з них. До сьогоднішнього дня даний метод – найбільш універсальний серед всіх існуючих, за умови що нам відомо тип алгоритму та принцип його роботи, при цьому не важко здогадатись, що ККД даного методу є вкрай низьким.

Для оцінки реальності загрози атаки грубої сили вводиться термін «практичний час», як деяка відповідність теоретичному часу, за який машина прогнозовано зможе підібрати ключ, до часу збереження актуальності та цінності прихованої інформації. Простіше кажучи, якщо умовна Єва перехопила зашифроване повідомлення компанії конкурента, і на атаку грубої сили, прогнозовано буде затрачено 50 років, то такий час можна вважати непрактичним, адже за 50 років розшифроване повідомлення дасть Єві мінімум користі. При цьому обов'язково слід врахувати той факт, що якщо на сьогоднішній день прогнозований час атаки й складатиме 50 років, то абсолютно не факт, що через кілька років, з урахуванням нових технологій та потужностей, цей час не складатиме 50 годин, чи навіть хвилин. Окрім цього на сьогоднішній день все більшої популярності набувають розподілені обчислення, що переганяють за швидкістю роботи навіть передові суперкомп'ютери [12].

Таким чином запас міцності, в контексті стійкості криптосистеми до атаки грубої сили, як одна з базових характеристик надійності шифру повинна враховувати не лише обчислювальні потужності, існуючі сьогодні, а і їх прогнозоване зростання, яке є неминучим.

Слід враховувати й безліч інших існуючих криптоатак, такий як, наприклад, атака на основі перехопленого відкритого тексту, атака на основі підібраного відкритого тексту, диференціальний криптоаналіз та інші існуючі підходи.

Головна сила запропонованої криптосистеми – нелінійність та рандомізація алгоритму, саме це і повинно забезпечити його високу криптостійкість. В цілому, ідея полягає у створенні кількох можливих варіантів роботи шифру на тому, чи іншому етапі його виконання, серед яких випадковим чином обирається один. Для можливості дешифрування, позначається лише індекс обраного варіанту, який не дає криптоаналітику жодної додаткової інформації про те, що за ним стоїть.

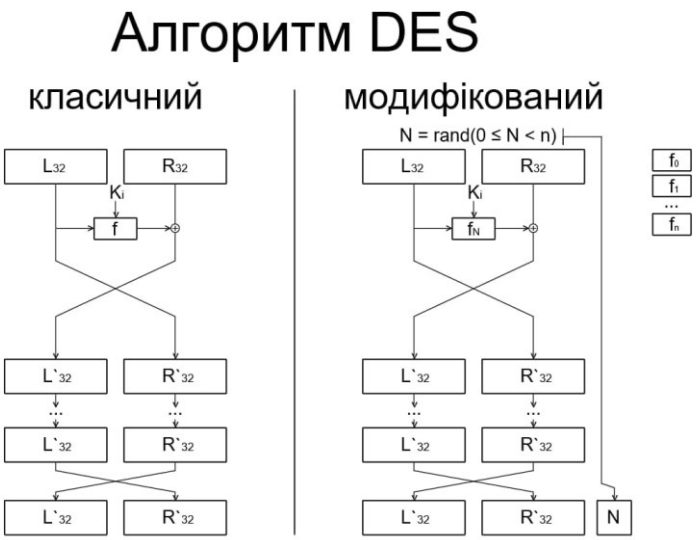


Рис. 1. Схема звичайного та модифікованого алгоритму DES

Даний підхід можна продемонструвати на прикладі алгоритму DES (Рис. 1).

В класичному представлені даного алгоритму у нас є одна функція, яка на основі раундового ключа та першого підблоку мережі Фейстеля, розміром 48 та 32 біта, відповідно, та повертає новий 32-бітний блок даних. Проте давайте змоделюємо ситуацію, при якій в даному алгоритмі у нас не одна функція, а, до прикладу, їх вісім. Кожна з цих функцій також прийматиме на вхід два блока у 48 та 32 біт та повертатиме, на їх основі, новий 32-бітний блок, при цьому кожна з них буде робити це по-різному. Якщо точніше, вони будуть і далі працювати за схемою класичної функції DES, проте, кожна з цих 8 функцій матиме деякі особливості: одна, наприклад, по-іншому розширюватиме вхідний блок, друга – перед розширенням проводитиме циклічний зсув вхідного блоку на деяке число, третя – проводитиме аналогічний зсув, але вже після розширення, четверта – залишиться у класичному вигляді, без змін, а п’ята – додаватиме 27, за модулем 256, до кожного парного байту після розширення вхідного блоку і так далі. Як результат – кожна функція, в цілому, подібна до інших та кожну з них можна без проблем замінити іншою, проте 32-бітні блоки які буде повертати та, чи інша функція, як правило, будуть різні.

Тепер нам залишається лише незначно модифікувати загальний алгоритм шифрування: при генерації ключа, додатково, випадковим чином цим функціям буде присвоєно індекси від 0 до 9. Інформація про дані індекси та їх відповідності буде частиною секретного ключа. А при шифруванні, перед першим раундом кожного блоку, ми обиратимемо випадкове ціле число в діапазоні $[0; 8)$, яке і вказуватиме яку функцію з переліку ми використовуватимемо у наступних 16 раундах. Інформацію про те яка функція була використана можемо записати у вигляді 3-бітної комбінації в кінці, після зашифрованого 64-бітного блоку.

При такій модифікації алгоритму шифрований текст розшириться на n біт, де $n = \frac{N_{\text{повідомлення}} \times 67}{64}$, тобто, приблизно, на 4,5%.

В описаному випадку, при перехопленні шифрованого повідомлення, у криптоаналітика будуть на руках самі шифроблоки, а також індекси використаних функцій, без будь-якої важливої інформації, звичайно, якщо криптоаналітик знає принцип роботи даної модифікації. Проте в даній ситуації спеціаліст зможе однозначно сказати чи однакові функції були використані, в тому, чи іншому випадку, чи ні, елементарно зрівнявши ці самі індекси вкінці блоків. На основі даної інформації він зможе згрупувати блоки, в яких були використані однакові функції та досліджувати їх окремо.

Для того щоб позбавити криптоаналітика такої можливості, введемо ще одну зміну: індексів буде більше ніж самих функцій. На описаному вище прикладі, це можна зробити двома шляхами: або зменшити кількість функцій, тоді в нас буде, наприклад, 4 функції та 8 індексів, або збільшити кількість індексів, тоді при 8 функціях ми матимемо 16 індексів.

При генерації нового ключа, як і раніше, ми випадково генеруємо та записуємо відповідності між функціями та індексами, проте вже не у відношенні 1:1, а у відношенні 1:m, де одній функції відповідатиме кілька індексів. При шифруванні тепер ми кидатимемо монетку двічі: перший раз – щоб вибрати функцію, другий – щоб обрати один індекс, серед всіх, пов'язаних з даною функцією.

Слід зазначити що дані числа краще обирати рівним 2^n, а кількість функцій, рекомендовано, має бути кратною кількості індексів, при чому вони повинні бути рівномірно розподілені між функціями. Це дозволить в повній мірі, без надлишковості, використовувати діапазон значень, при шифруванні, а також забезпечить однакову ймовірність випадання функцій.

Тепер, перехопивши повідомлення, криптоаналітик не зможе однозначно сказати чи були використані однакові функції в блоках з різними індексами, адже це може бути як інший ідентифікатор тієї ж самої функції, так й ідентифікатор іншої функції.

Також звідси витікає цікава властивість даного алгоритму: зашифрувавши одне і те ж саме повідомлення, використовуючи один і той ж самий ключ, ми отримаємо різні шифротексти, оскільки тепер те як буде зашифровано той чи інший блок, залежатиме від випадкового показника, при шифруванні. Отже, криптоаналітик, перехопивший n зашифрованих повідомлень, не зможе однозначно виявити які серед них будуть ідентичними після дешифровки.

Приклад, наведений на основі криптографічного алгоритму DES, наглядно та в повній мірі демонструє принципи роботи, на базі яких пропонується створити окрему криптосистему.

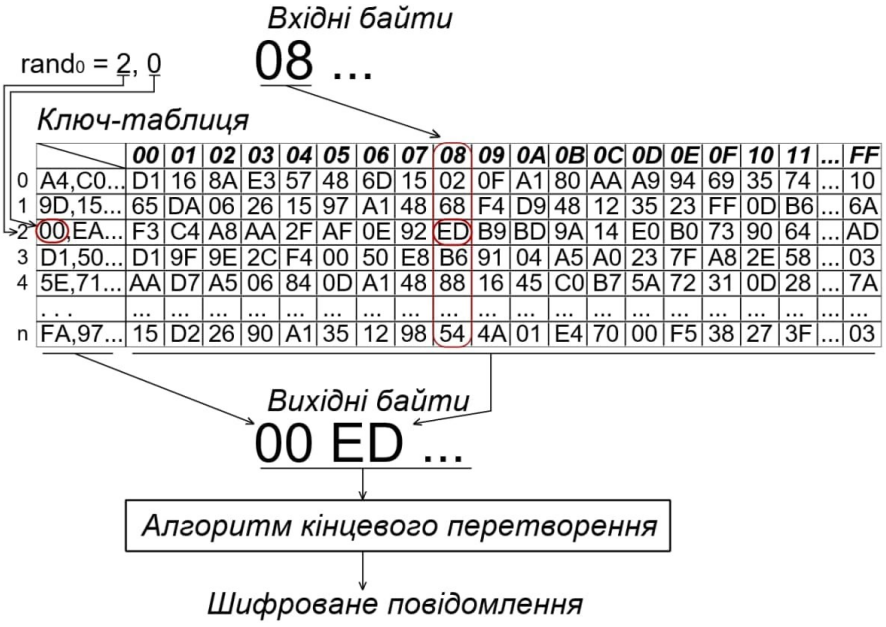
Навіть у вигляді модифікації до вже існуючого алгоритму, така нелінійність, наявність кількох «сценаріїв» роботи, серед яких обирається випадковий, дозволяє значно ускладнити роботу криптоаналітиків та понизити ефективність машинного криптоаналізу. Причому слід зазначити, що в описаній модифікації зазначена варіативність була додана лише для раундових функцій, хоча це зовсім не єдиний аспект, де даний підхід можна було б застосувати, навіть у випадку шифру DES.

Таким чином, аналогічно до наведеного прикладу ми можемо спроектувати окремий алгоритм, в якому описаний принцип нелінійності буде не модифікацією, а основою його роботи.

Логікою шифрування в даному алгоритмі буде заміна одного байту на інший, відповідно до деякої поліалфавітної таблиці перестановок. Дана таблиця міститиме в собі n рядків та 256 стовпців, якщо за умовний блок даних ми візьмемо один байт. В кожному рядку буде послідовність від 0 до 255, перемішана випадковим чином. Кількість рядків, а відповідно «алфавітів перестановки», може бути якою завгодно.

Кожному рядку, точно як і функції, у прикладі з DES, присвоюється m випадкових двійкових ідентифікаторів. Розрядність цих ідентифікаторів також може бути обрана різна, проте вона повинна бути однаковою для всіх ідентифікаторів. Від обраної розрядності залежатиме, по-перше, кількість алфавітів, яку ми можемо визначити, наприклад якщо розрядність дорівнюватиме двом, то максимум у нас може бути 4 алфавіти, а з урахуванням рекомендації використовувати не менше двох ідентифікаторів на один алфавіт – всього 2. По-друге, від розрядності залежатиме те, наскільки збільшиться шифрований текст, порівняно з вхідним повідомленням. Якщо розрядність ідентифікатора буде рівною розрядності нашого блоку даних, а у нашому випадку – це 8 біт, то шифроване повідомлення буде вдвічі більше за вхідне. Чим менша розрядність ідентифікатора, по відношенню до розміру блоку даних, тим менше буде збільшення вихідного повідомлення при шифруванні і навпаки.

Дана таблиця замін, разом із відповідними ідентифікаторами, складатиме собою секретний ключ. Для її компактного запису можна використовувати різноманітні технології стиснення.



	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	...	FF
0	A4,C0...	D1	16	8A	E3	57	48	6D	15	02	0F	A1	80	AA	A9	94	69	35	74	...	10
1	9D,15...	65	DA	06	26	15	97	A1	48	68	F4	D9	48	12	35	23	FF	0D	B6	...	6A
2	00,EA...	F3	C4	A8	AA	2F	AF	0E	92	ED	B9	BD	9A	14	E0	B0	73	90	64	...	AD
3	D1,50...	D1	9F	9E	2C	F4	00	50	E8	B6	91	04	A5	A0	23	7F	A8	2E	58	...	03
4	5E,71...	AA	D7	A5	06	84	0D	A1	48	88	16	45	C0	B7	5A	72	31	0D	28	...	7A
. . .	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
n	FA,97...	15	D2	26	90	A1	35	12	98	54	4A	01	E4	70	00	F5	38	27	3F	...	03

Рис. 2. Схема шифрування

Схема шифрування даним методом показана на рис. 2 та в цілому подібна до описаної на прикладі DES: спочатку ми обираємо два випадкових числа, з яких перше – в діапазоні $[0; n)$, де n – кількість алфавітів, а друге – в діапазоні $[0; m)$, де m – кількість ідентифікаторів, відповідних даному алфавіту. Після цього ми заміняємо вхідний блок даних на вираз, що складається з обраного ідентифікатора та числа, що знаходиться в обраному алфавіті на позиції, номер якої відповідає числу, утвореного з блока вхідних даних. Тобто, якщо ми шифруємо 8-бітні блоки, і на вході, як приклад, отримали блок «10001010», що у десятковій формі відповідає числу 138, а випадкові числа випали 2 і 0, за умови, що вони відповідатимуть межам зазначених діапазонів, то шифрований вираз для даного блоку складатиметься з 0-го ідентифікатора 2-го алфавіту перестановок та числа, що знаходиться на 138-й позиції у 2-му алфавіті. Такі перетворення почергово проводяться для кожного блоку даних, до кінця відкритого повідомлення.

В прикладі з DES на цьому ми закінчували, проте в даному випадку не слід залишати шифроване повідомлення в такому вигляді, оскільки у обізнаного криптоаналітика, при перехопленні буде можливість проаналізувати однакові ідентифікатори та відповідно, на основі великої кількості повідомлень скласти деяку кореляцію. Щоб позбавити його такої можливості, ми використаємо два прийоми.

По-перше, ми додамо варіативності до принципу зчеплення ідентифікатора та блоку заміни. Це дозволить ускладнити розпізнавання ідентифікаторів та ускладнить криптоаналіз. Приклади зчеплень елементів продемонстровано на рис. 3.

По-друге, після формування вихідного масиву байт, після завершення замін, ми «змішаємо» його за допомогою алгоритму кінцевого перетворення. Найпростішим варіантом даного алгоритму може бути поблокове додавання за модулем 2, в режимі зчеплення блоків, де ключ та перший блок деяким чином формуються на основі таблиці. Даний алгоритм може бути реалізовано на основі мережі Фейстеля з невеликою кількістю раундів, на основі матричних перестановок, чи на основі будь-якого іншого існуючого алгоритму, що забезпечує надійне «розмиття».

Таким чином даний алгоритм буде стійким до атаки грубою силою, оскільки простим перебором відновити таблицю замін не можливо за практичний час, а за необхідності, розмір вхідного блока даних можна додатково збільшити. Кількість можливих варіантів перестановок для одного 8-бітного алфавіту складає 256!, а за умови що алфавітів багато, кількість можливих комбінацій забезпечує надійність ключа навіть з урахуванням розвитку технологій.

Слід зауважити, що при абсолютно випадковій генерації ключа, шифротекс, звісно, також вийде випадковий. При цьому, ми можемо піти від зворотнього: припустимо що в нас вже є шифротекст, який ми маємо отримати. Ми можемо згенерувати такий ключ, щоб при шифруванні конкретним способом, без викидання випадкових чисел, ми отримали необхідний нам шифротекст. При даному підході також з'являються додаткові вимоги до алгоритму кінцевого перетворення: він повинен мати змогу розшифрувати будь-який випадковий масив байт.

Рис. 3 Приклади зчеплення ідентифікатора та блоку заміни

Нелінійність алгоритму ускладнить машинний та людський криптоаналіз та затруднить статистичні дослідження.

Даний алгоритм також буде стійким на до атаки на основі відкритого тексту, оскільки, маючи на руках відповідне шифроване повідомлення, криптоаналітик матиме лише один з можливих варіантів шифротексту, при цьому криптоаналітик не матиме доступу до всіх інших можливих варіантів шифрування.

В цілому запропонований алгоритм представляє собою цікавий та перспективний метод криптографічного захисту, безумовно потребуючи розвитку та подальших досліджень. Окрім криптографічного, даний алгоритм представляє також стеганографічний інтерес, оскільки нелінійність, яка породжує варіативність шифротекстів, дозволяє, фактично, один і той ж самий байт зашифрувати десятками, або навіть сотнями комбінацій. Виходячи з цього, теоретично, можливо створити такий ключ, при якому деякий конфіденційний текст в зашифрованому вигляді представлятиме інший осмислений текст, що не викликатиме підозр. Даний аспект також потребує додаткових досліджень.

Висновки

Таким чином, алгоритми шифрування, що мають в собі елементи нелінійності, включають рівноможливі варіанти виконання, серед яких в процесі виконання обирається один, значно підвищують його стійкість та захищенність.

Запропонований алгоритм, який в повній мірі відповідає описаним принципам, проявляє цікаві властивості, а проведенні дослідження говорять про його достатню захищеність та стійкість.

Безумовно, наведені алгоритми потребують додаткового вивчення, проте вже на даному етапі можна говорити про те, що навіть модифікація вже існуючих алгоритмів, введення в них варіативних елементів, є легким способом підвищення їх надійності.

Окрім зазначеного, даний алгоритм може знайти розвиток у сфері стеганографії.

Літертура

1. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

2. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

3. Основы криптографии/ Г.В. Басалова. – М.: ИНТУИТ, 2016. - 283 с.

4. Cryptology and information security - past,present, and future role in society/ S. Bhattacharya. - International Journal on Cryptography and Information Security (IJCIS). – Vol. 9, No.1/2, 2019. – P. 13-36.

5. Муляр І.В. Ітераційно-геометричний метод для стійкого перцептуального хешування зображення / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 1. – С. 76–79

6. Hybrid cryptographic technique using rsa algorithm and scheduling concepts/ M. Shankar, P. Akshaya// International Journal of Network Security & Its Applications (IJNSA)/ Vol.6, No.6. – 2014. - p. 39-48

7. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. – 558 с.

8. Digital Watermarking and Steganography: Fundamentals and Techniques / Edited by Frank Y. Shih**. –** Taylor & Francis Group, 2017**. –** 293 p

9. The Evolution of Cryptology [Електронний ресурс]/ G. R. Souza. – California State University, San Bernardino, 2016. – режим доступу: https://core.ac.uk/reader/55336770

10. Cryptology and communication security [Електронний ресурс]/ Shri Kant. – Defense Science Journal. – Vol. 62. - №1. – режим доступу: https://core.ac.uk/reader/333719963

11. Криптоанализ шифрсистемы ACBF/ И. В. Боровкова, И. А. Панкратова. – Прикладная дискретная математика. Приложение, Томск. – 2019. – С. 90-93.

12. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей./ В.М. Франчук – К.: НПУ імені М.П. Драгоманова, 2014. – 120 с.

References

1. Informatsiina bezpeka: navchalnyi posibnyk / [Iu. Ya. Bobalo, I. V. Horbatyi, M. D. Kiselychnyk, A. P. Bondariev ta in.]; za zah. red. d-ra tekhn. nauk, prof. Yu. Ya. Bobala ta d-ra tekhn. nauk, dots. I. V. Horbatoho. – Lviv: Vydavnytstvo Lvivskoi politekhniky, 2019. – 580 s.

2. Prykladna kryptolohiia: systemy shyfruvannia : pidruchnyk / O. H. Korchenko, V. P. Sidenko, Yu. O. Dreis. – K. : DUT, 2014. – 448 s.

3. Osnovы kryptohrafyy/ H.V. Basalova. – M.: YNTUYT, 2016. - 283 s.

4. Cryptology and information security - past,present, and future role in society/ S. Bhattacharya. - International Journal on Cryptography and Information Security (IJCIS). – Vol. 9, No.1/2, 2019. – P. 13-36.

5. Muliar I.V. Iteratsiino-heometrychnyi metod dlia stiikoho pertseptualnoho kheshuvannia zobrazhennia / V. M. Dzhulii, Yu. P. Klots, I. V. Muliar, V. M. Cheshun // Herald of khmelnytskyi National University. – 2020. – № 1. – S. 76–79

6. Hybrid cryptographic technique using rsa algorithm and scheduling concepts/ M. Shankar, P. Akshaya// International Journal of Network Security & Its Applications (IJNSA)/ Vol.6, No.6. – 2014. - p. 39-48

7. Kompiuterna stehanohrafichna obrobka y analiz multymediinykh danykh: pidruchnyk. / H. F. Konakhovych, D. O. Prohonov, O. Yu. Puzyrenko. – Kyiv: «Tsentr uchbovoi literatury», 2018. – 558 s.

8. Digital Watermarking and Steganography: Fundamentals and Techniques / Edited by Frank Y. Shih. – Taylor & Francis Group, 2017. – 293 p

9. The Evolution of Cryptology [Elektronnyi resurs]/ G. R. Souza. – California State University, San Bernardino, 2016. – rezhym dostupu: https://core.ac.uk/reader/55336770

10. Cryptology and communication security [Elektronnyi resurs]/ Shri Kant. – Defense Science Journal. – Vol. 62. - №1. – rezhym dostupu: https://core.ac.uk/reader/333719963

11. Kryptoanalyz shyfrsystemы ACBF/ Y. V. Borovkova, Y. A. Pankratova. – Prykladnaia dyskretnaia matematyka. Prylozhenye, Tomsk. – 2019. – S. 90-93.

12. Zakhyst informatsiinykh resursiv: kryptohrafichni ta stehanohrafichni metody zakhystu danykh. Posibnyk dlia vykladachiv, vchyteliv ta studentiv informatychnykh spetsialnostei./ V.M. Franchuk – K.: NPU imeni M.P. Drahomanova, 2014. – 120 s.

Надійшла / Paper received : 12.11.2020 р. Надрукована/Printed :04.01.2021 р.