УДК: 004.056.55

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ

Метьолкін А.О., Кардашук В.С

RESEARCH METHODS TO IMPROVE CRYPTOGRAPHIC STABILITY

Metyolkin A.O., Kardashuk V.S.

У статті розглянуто питання щодо надійності криптографічних алгоритмів шифрування, застосування спеціальних методів теоретичного і експериментального характеру. Виконано огляд основних методів шифрування та засоби їх удосконалення

Ключові слова: *криптографія, криптоаналіз, ключі шифрування, алгоритм, цифровий підпис.*

Вступ. Криптографія - наука про методи забезпечення конфіденційності та збереження цілісності даних. На сучасному етапі розвитку інформаційних технологій актуальним є питання подальших досліджень криптостійкості симетричних і асиметричних алгоритмів та алгоритмів, заснованих на хеш-функціях.

Постановка проблеми. При значній кількості методів та алгоритмів шифрування дослідження в області криптоаналізу є невід'ємною частиною криптографії. У даній роботі за допомогою практичного методу моделювання алгоритмів необхідно провести аналіз алгоритмів шифрування/дешифрування відносно їх стійкості на основі існуючих методів та надати рекомендації щодо їх практичного застосування.

Аналіз останніх досліджень і публікацій. У роботі [1] проаналізована робота алгоритмів шифрування та постановка питання щодо криптостійкості алгоритмів шифрування із відкритими та закритими ключами. У [2] розглянуті теоретичні матеріали по методам шифрування, такі як первинні характеристики криптоаналізу. У [3] розглянуто методи та стандарти реалізації алгоритму шифрування RSA, формули для розрахунків ключів шифрування, основні вимоги до алгоритмів шифрування та їх криптоаналіз.

Мета статті. Дослідження криптостійкості на прикладі алгоритму шифрування RSA.

Результати досліджень. Криптографія в першу чергу спеціалізується на методах шифрування інформації – шифрування первинного тексту за допомогою алгоритму або криптоключа в шифрований текст [4]. Зазвичай, криптографія базується на симетричних криптосистемах, в яких шифрування і розшифрування виконується на базі одного ключа. Також у криптографії використовуються асиметричні криптосистеми, а для підвищення стійкості шифрування використовують системи електронного цифрового підпису, хеш-функції, управління ключами, отримання прихованої інформації, квантова криптографія.

Одним із найпростіших варіантів для шифрування інформації є «шифр Цезаря» – заміна літер алфавіту на літери того ж алфавіту, але із зсувом на три позиції. Даний алгоритм дуже простий, з невеликим ступенем надійності шифрування. Щоб розшифрувати такий текст, досить знати алгоритм.

Існує й інший спосіб отримання шифрованого текст - замінити літери на літери іншого алфавіту або на символи. Щоб прочитати такий текст, потрібен ключ, який співвідносить ці алфавіти між собою. Створенням стійкого до частотного криптоаналізу шифру було досить серйозними питанням. Наприклад, застосування декількох алфавітів і т. п. Подібні алгоритми шифрування дали основу для більш сучасних криптосистем.

Принцип Керкгоффса, говорить: «Стійкість криптосистеми не повинна залежати від секретності алгоритму». Тобто передбачається, що зловмисник знає, якимось чином відкритий текст (текст до шифрування). Але ключ, за допомогою якого це робиться, повинен залишатися таємницею. Зламати таку систему можна простим перебором ключа, саме тому важливо, щоб ключ був не надто коротким і щоб був один-єдиний спосіб зрозуміти, що він правильний. У той же час занадто великий ключ забирає досить великий відсоток обчислювальних ресурсів, навіть для сучасних комп'ютерів.

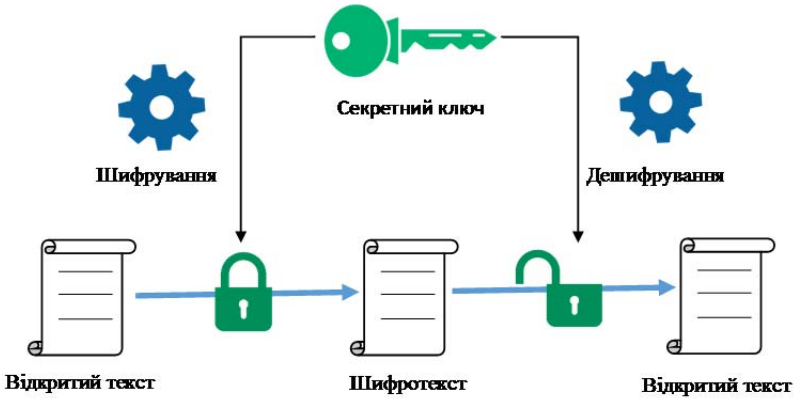

Рис. 1. Принцип роботи симетричного шифрування на основі ключа

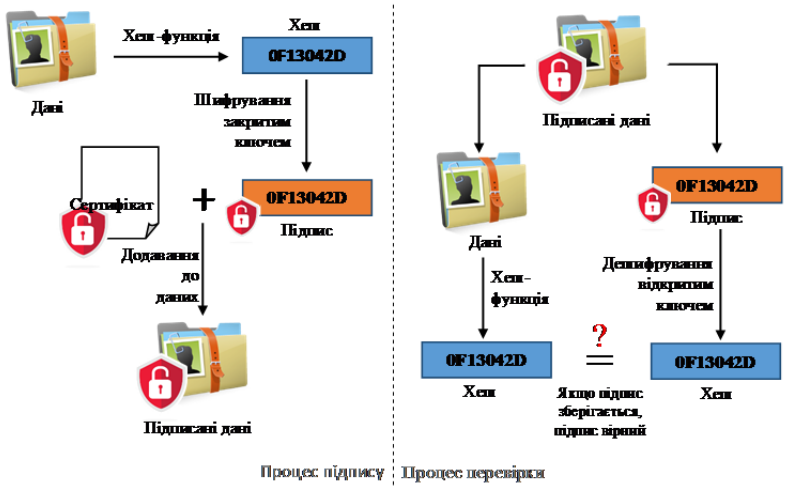

Рис. 2. Принцип роботи цифрового підпису

Наприкінці 70-х років минулого століття інтерес до криптографії зріс як у держслужб, так і у звичайних користувачів. Так, алгоритм RSA набув широкої популярності та використання в криптосистемах. Алгоритм RSA володіє криптографічними властивостями, що притаманні симетричним системам шифрування. У симетричній криптографії для шифрування і дешифрування використовується один ключ. Ці прості алгоритми ідеологічно описані ще в 50-х роках минулого століття, але всім їм властивий один великий недолік, а саме необхідність захищеного каналу для передачі ключа шифрування. Цю проблему симетричного шифрування називають проблемою поширення ключів [6].

Дешифрування - зворотний процес шифрування. На основі ключа шифрований текст перетвориться у вихідний [7].

Для іншого способу шифрування застосовується пара ключів: відкритий і закритий, так званий секретний. Відкритий і закритий ключі дозволяють криптографічним алгоритмам шифрувати/дешифрувати повідомлення. При цьому повідомлення, зашифровані відкритим ключем, розшифрувати можна тільки за допомогою закритого ключа. Відкритий ключ публікується в сертифікаті власника і доступний вже при підключенні клієнта, а закритий – зберігається у власника сертифіката.

Відкритий і закритий ключ між собою пов'язані математичними залежностями, тому підібрати відкритий або закритий ключ неможливо за короткий час. Перевірити, чи не була інформація спотворена під час передачі по зашифрованому каналу можна за допомогою електронного цифрового підпису (digital signature)[8]. В цьому випадку текст зашифрований закритим ключем і разом з відкритим текстом відправляється відправнику. Якщо розшифрування проводити відкритим ключем і текст співпадає з не зашифрованим текстом, то проведена дешифрація є успішною. На практиці закритим ключем, зазвичай, зашифрована хеш-функція документа. Електронний підпис крім іншого містить так званий сертифікат відкритого ключа, виданий довіреним центром сертифікації (CA, certification authority), який має дані по всіх відкритих ключах та їх користувачах. Сертифікат теж повинен бути підписаний. Важливо,

що відкритий ключ довіреного центру повинен бути відомий заздалегідь, інакше його теж можна підробити.

Криптографічно стійка хеш-функція перетворює вихідний текст в один рядок так, що з цього рядка неможливо (або дуже складно) отримати вихідний текст. Хеш-функцію використовують, наприклад, там, де потрібно вводити пароль: фразу в рядку введення порівнюють не з самим паролем, а з його хеш-функцією.

Хеш-функція-перетворення тексту довільної довжини в текст фіксованої довжини визначається як

$$H = hash(P), \tag{1}$$

де P - пароль (відкритий текст), довжина P від 0 до нескінченності;

H-хеш (хешований текст), довжина $H = N$ біт (за умови що функція hash повертає хеш-значення довжиною N біт).

Для посилення криптографічної стійкості використовують ітераційний алгоритм отримання ключів.

Ключі знаходяться за наступним алгоритмом:

$$\begin{aligned} &K1 = hash(password) \\ &K2 = f(K1) \\ &... \\ &K(n) = f(K(n-1)) \end{aligned} \tag{2}$$

де f –функція по перетворенню ключа. Якщо знати $K1$, то можливо обчислити всі інші Ki, $i = 2..n$.

Зловмисник не знаючи початкового хеш-паролю, але знаючи значення хеш функції може розшифрувати весь текст. Для підбору пароля методом звичайного перебору, повинен зробити підбір 2^S значень (S-розмір хеш-значення в бітах). Якщо хеш-функція повертає значення довжиною 64 біта-потрібно зробити перебір 2^{64} = 8 446 744 110 значень.

Комп'ютер зловмисника може перебирати 1000000 паролів в секунду. Тоді підбір хеш-значення максимально займе 213 503 982 днів.

Якщо використовувати метод злому шифрів або пошуку колізій хеш-функцій, тоді кількість варіантів скоротиться в середньому вдвічі – $2^{64}/2$ = 4 294 967 296 значень. На перебір цих значень піде всього лише 1,2 години.

Найуразливіше місце криптографічного захисту - це людина. Зламувати шифри також є частиною криптографії, якою займається криптоаналіз. Криптологія об'єднує як науку шифрування, так і дешифрування

Перевіримо на практиці надійність ключів шифрування за допомогою програми Cryptotool 2 [10], що працює з шифрами, та допомагає змоделювати систему шифрування.

Cryptotool 2 підтримує усі відомі на сьогодні моделі шифрування. Функціональні блоки мають модулі для введення і виведення інформації в процесі роботи, які в свою чергу можуть приєднуватися до інших функціональних блоків і обмінюватися інформацію між собою. Кожен блок має сценарій роботи і віртуалізації. Це дає можливість після складання всієї схеми запустити моделювання роботи. Після запуску моделювання кожен з блоків починає поступове завантаження з відображенням процесу у вигляді процентного виконання. По закінченню циклу на кожному блоці а також у вікні процесу відображається повний хід дій, в якому можуть бути присутні помилки та не стикування блоків у разі помилки при передачі інформації.

Одним з найбільш поширених методів несиметричного шифрування/дешифрування є метод шифрування з відкритим ключем на основі алгоритму RSA, що заснований на використанні операції піднесення до степеню модульної арифметики. Алгоритм RSA можна представити у вигляді наступної послідовності для отримання ключів шифрування:

$$n = pq, \tag{3}$$

де p i q - два великих простих числа[5].

На практиці для забезпечення криптостійкості системи величина цих чисел повинна бути довжиною не менше двохсот десяткових розрядів.

n - відкрита компонента ключа.

$$f(p,q) = (p-1)(q-1), \tag{4}$$

де $f(p,q)$ - функція Ейлера.

$$e * d(|f(p,q)|) = 1, \tag{5}$$

де e - число, яке має бути взаємно простим із значенням функції Ейлера і меншим, ніж f (р q.) d – число, яке задовольняє співвідношенню.

Числа e і n приймаються в якості відкритого ключа. В якості секретного ключа використовуються числа d і n.

Підберемо три варіанти для значень p та q , та розрахуємо параметри закритого і відкритого ключа (табл. 1).

Таблиця 1

Обчислені ключі шифрування

Параметри p,q	Відкриті ключі	Закриті ключі
251,31	83,7781	4247,7781
1523,113	251,172099	29203,172099
165173,1231	647,203327963	67511183,203327963

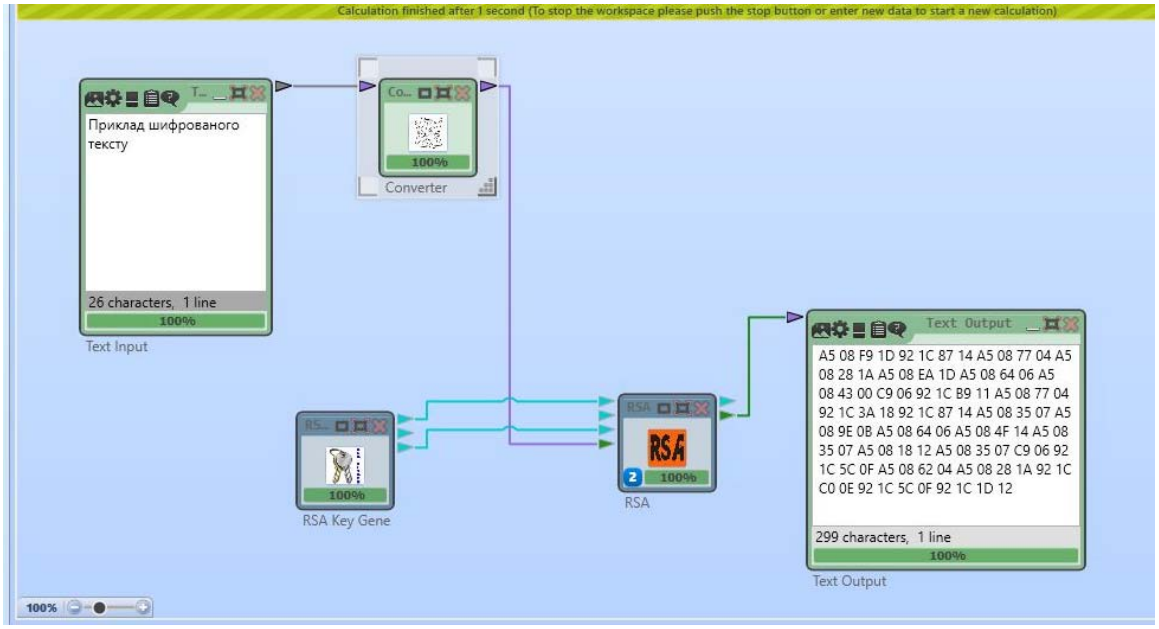

Рис. 3. Вікно програми Cryptotool 2.1 з функціональною схемою

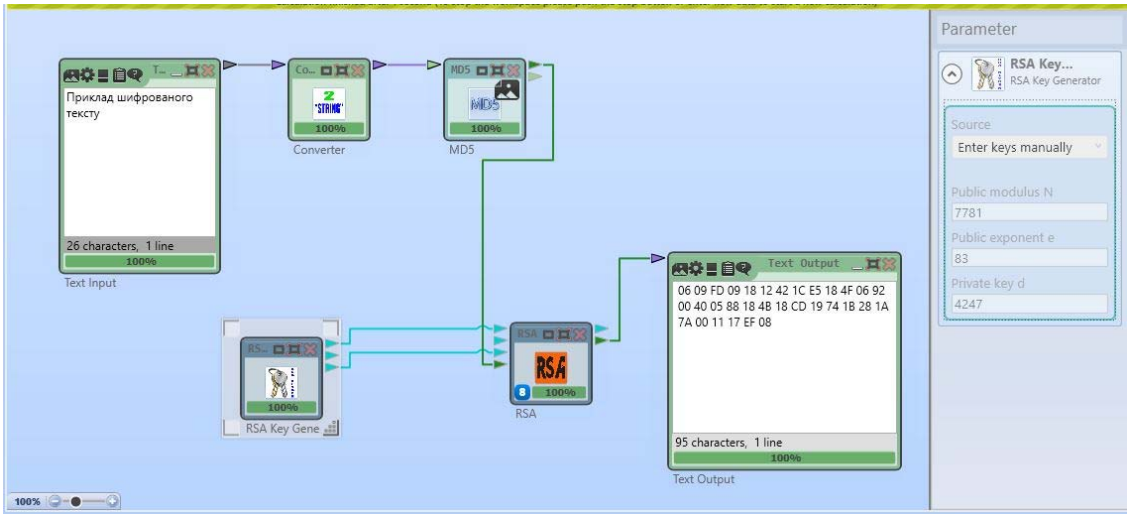

Рис. 4. Шифрування із застосуванням хеш-функції MD5 у програмі Cryptotool 2

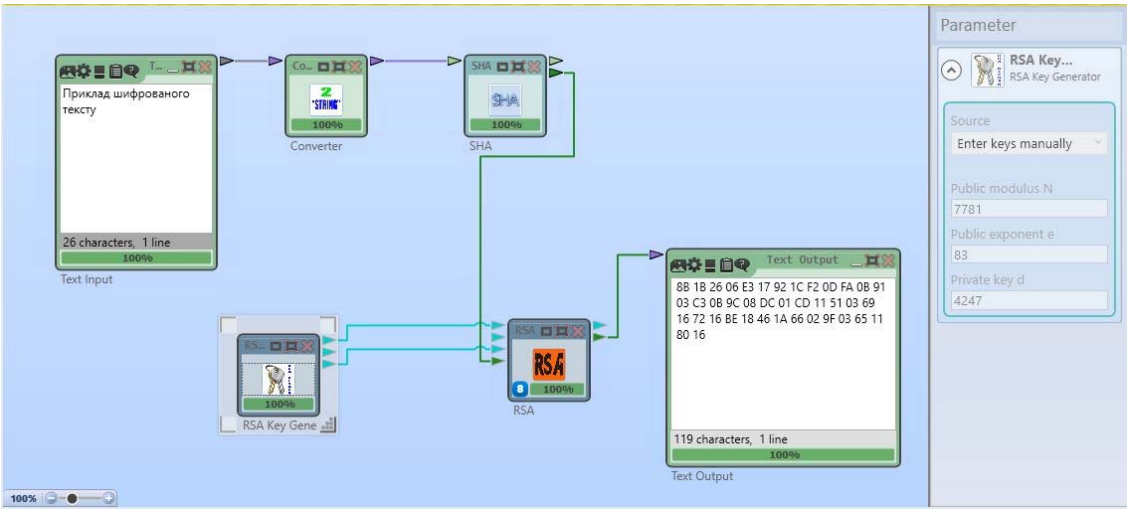

Рис. 5. Шифрування з хеш-функцією SHA-1 у програмі Cryptotool 2

Розраховані данні занесені до програми та проведений процес шифрування.

Отримані результати дослідження алгоритмів наведені в табл. 2.

Таблиця 2

Значення для шифрування з першим набором ключів(83,7781; 4247,7781)

Алгоритм хеш-функції	Кількість символів
RSA	299
MD5	95
SHA-1	119
SHA-256	191
SHA-512	383

Для аналогічних моделей з іншими наборами ключів отримані такі значення (табл. 3,4).

Таблиця 3

Значення для шифрування з другим набором ключів(251,172099; 29203,172099)

Алгоритм хеш-функції	Кількість символів
RSA	303
MD5	101
SHA-1	123
SHA-256	213
SHA-512	391

Таблиця 4

Значення для шифрування з третім набором ключів (647,203327963; 67511183,203327963)

Алгоритм хеш-функції	Кількість символів
RSA	307
MD5	101
SHA-1	130
SHA-256	197
SHA-512	401

На рис. 6 наведена залежність шифрованих символів від розміру ключа

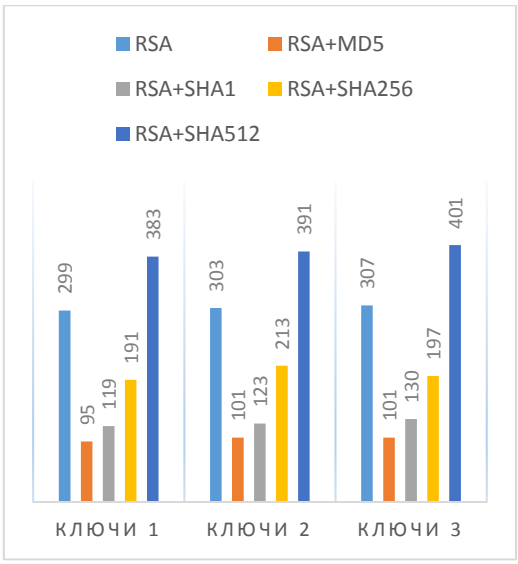

Рис. 6. Залежність шифрованих символів від розміру ключа

З рис. 6 видно, що при збільшенні розміру ключа найбільших змін отримує алгоритму RSA з використанням SHA-512. Порівняльні дані діаграми показують ефективність використання алгоритмів шифрування в цілому. Як висновок, можна зазначити, що при умові обмеженої пам'яті комп'ютера використання хеш-функції RSA + MD5 є найбільш доцільним.

При використанні алгоритму RSA отриманий шифротекст є в 10 разів більший на відміну від початкового тексту, але його стійкість є низькою. Слід зазначити, що разом із збільшенням розміру ключів шифрування збільшується і надійність даної системи, тобто чим більш опрацьовані первинні даних та ключі для шифрування, тим більша його криптостійкість.

Висновки. У статті розглянуті основні алгоритми і методи шифрування та питання щодо підвищення їх криптостійкості .

Для дослідження обрано алгоритм RSA та розглянуто етапи його роботи, взаємодія із ключами шифрування.

В ході досліджень виявлено, що надійність алгоритму залежить від ключів шифрування, а також ступеня його опрацювання. Розглянуті принципи підвищення криптостійкості на прикладі ітераційного методу та хеш-функцій, які впливають на дані шифрування, що посилює загальну криптостійкість методу та зменшує ризик атак звичайними методами злому.

Література

1. С. Гнатюк, В. Кінзерявий, А. Охріменко. Особливості криптографічного захисту державних інформаційних ресурсів - Безпека інформації. - 2012. - № 1. - С. 68.
2. І.В. Лисенко, Ю.В. Трегуб . Порівняльна характеристика можливостей програмних платформ і мов програмування з точки зору реалізації криптоалгоритмів - Системи управління, навігації та зв'язку. – 2017- випуск 1(41).
3. J. Gallier,J. Quaintance. Notes on Primality Testing And Public Key Cryptography Part1.
4. Алферов А.Ю. Основы криптографии./ Алферов А.Ю., Зубов А.С. – М.: Наука, 2004- 423с.
5. Герман О.Н. Теоретико - числовые методы в криптографии / О.Н. Герман, А.Ю. Нестеренко. — М., 2012. — 300 с.
6. Бабаш А.В. История криптографии / Бабаш А.В., Шанкин Г.П Часть I. — М.: Гелиос АРВ, 2002. — 240 с.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
8. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000- 150 с.
9. Аграновский А.В Практическая криптография. Алгоритмы и их программирование / Аграновский А.В., Хади Р.А../ — М: Солон-Пресс, 2009. — 258 с.

10. Downloads - CryptoTool Portal. Режим доступу https://www.cryptool.org/de/ct2-downloads (дата звернення 17.09.2018).

R e f e r e n c e s

1. S. Hnatyuk, V. Kinesberyev, A. Okhrimenko. Features of Crypto protection of Information Technologies - 2012. - No. 1. - P. 68.
2. I.V. Lysenko, Y.V. Tregub Comparative characteristics of the capabilities of software platforms and programming languages in terms of the implementation of cryptographic algorithms - Control systems, navigation and communication. - 2017- Issue 1 (41).
3. J. Gallier, J. Quaintance Notes on Primality Testing and Public Key Cryptography Part1.
4. Alferov A.Yu. Fundamentals of cryptography. / Alferov A.Yu., Zubov A.S. - Moscow: Nauka, 2004- 423 p.
5. Herman ON Numerical methods in cryptography / O.N. Herman, A.Yu. Nesterenko. - M., 2012. - 300 p.
6. Babash A.V. History of cryptography / Babash AV, Shankin GP Part I. - M .: Helios ARV, 2002. - 240 p.
7. Romanets, Yu.V., Timofeev, PA, Shangin, V.F. Protection of information in computer systems and networks / Ed. V.F. Shangina. - 2nd ed., Pererab. and add. - M .: Radio and communication, 2001. - 376 p.
8. Petrov A. A. Computer security. Cryptographic methods of protection. - Moscow: DMK, 2000-150 p.
9. Agranovsky A.V. Practical cryptography. Algorithms and their programming / Agranovsky AV, Hadi R.A ../ - M: Solon-Press, 2009. - 258 p.
10. Downloads - CryptoTool Portal. Access mode https://www.cryptool.org/de/ct2-downloads (date of request 17.09.2018).

Кардашук В.С., Метелкин А.О., Исследование методов повышения криптографической устойчивости.

В статье рассмотрены вопросы надежности криптографических алгоритмов шифрования, применение специальных методов теоретического и экспериментального характера. Выполнен обзор основных методов шифрования и расссмотрены средства их улучшения.

***Ключевые слова**: криптография, криптоанализ, ключи шифрования, алгоритм, цифровая подпись.*

Kardashuk V.S., Metelkin A.O. Research methods to improve cryptographic stability.

The article deals with the reliability of cryptographic encryption algorithms, the application of special methods of theoretical and experimental nature. The analysis of the basic methods of encryption and the inspected means of their improvement are executed.

***Keywords:** cryptography, cryptanalysis, encryption keys, algorithm, digital signature.*

Метьолкін А.С. – магістр групи КІ-17дм кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету імені Володимира Даля, e-mail: artemtyz9@gmail.com
Кардашук В.С. – к.т.н, доцент кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету імені Володимира Даля, e-mail: kardashuk1@gmail.com

Рецензент: д.т.н., проф. ***Архипов О.Г.***

Стаття подана 12.10.2018