DOI 10.31891/2307-5732-2022-307-2-46-52
УДК 004.056

СМІРНОВА Т. В.
https://orcid.org/0000-0001-6896-0612 e-mail: sm.tetyana@gmail.com
ЯКИМЕНКО Н. М.
https://orcid.org/0000-0002-4498-0093 e-mail: yakimenko_n_m@ukr.net
СМІРНОВ О. А.
https://orcid.org/0000-0001-9543-874x e-mail: dr.SmirnovOA@gmail.com
ПОЛІЩУК Л. І.
https://orcid.org/0000-0001-5093-1581 e-mail: pli_80@ukr.net
СМІРНОВ С. А.
Центральноукраїнський національний технічний університет
https://orcid.org/0000-0002-7649-7442 e-mail: smirnov.ser.81@gmail.com

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ СТІЙКОСТІ ТА ШВИДКІСНИХ ХАРАКТЕРИСТИК ЗАПРОПОНОВАНОЇ ФУНКЦІЇ ГЕШУВАННЯ УДОСКОНАЛЕНОГО МОДУЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

У роботі проведено дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах управління технологічними процесами. Об'єктом дослідження є процес забезпечення конфіденційності даних в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. Предметом є дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Метою даної роботи є дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування та гешування, а також синхронізація секретного ключа. У якості функцій шифрування та гешування можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведено експериментальне дослідження, що підтвердило криптостійкість удосконаленого алгоритму до лінійного та диференціального криптоаналізу та дозволило визначити, що швидкість криптографічної обробки даних удосконаленим методом з використанням розробленої функції шифрування є у 1,98 разів вищою у порівнянні з аналогами, а швидкість генерування ключів є вищою відповідно у 1,17 разів в порівнянні з генераторами, що використовуються зокрема в обраному прототипі.

Ключові слова: статистична стійкість, швидкісні характеристики, функція хешування, криптографічний захист, інформаційно-комунікаційна система.

TETIANA SMIRNOVA, NATALIIA YAKYMENKO, OLEKSII SMIRNOV,
LIUDMYLA POLISHCHUK, SERHII SMIRNOV
Central Ukrainian National Technical University

STUDY OF STATISTICAL STABILITY AND FAST CHARACTERISTICS OF THE PROPOSED HASHING FUNCTION OF THE IMPROVED CRYPTOGRAPHIC MODULE IN INFORMATION AND COMMUNICATION SYSTEMS

The study of statistical stability and speed characteristics of the proposed hashing function of the advanced module of cryptographic protection of information, which by recording information about the user ID, session ID, sending time, message length and its serial number, as well as using a new session key for encryption , allows to ensure the confidentiality and integrity of data in information and communication systems management processes. ***The object of research*** *is the process of ensuring the confidentiality of data in information and communication systems management systems based on cloud technologies.* ***The subject*** *is the study of statistical stability and speed characteristics of the proposed hashing function of the advanced module of cryptographic protection in information and communication systems.* ***The purpose*** *of this work is to study the statistical stability and speed characteristics of the proposed hashing function of the advanced module of cryptographic protection in information and communication systems for process control based on cloud technologies. To use this module effectively, it is important to choose crypto-resistant encryption and hashing methods, as well as secret key synchronization. Cryptoalgorithms resistant to linear, differential, algebraic, quantum and other known types of cryptanalysis can be used as encryption and hashing functions. An experimental study was conducted, which confirmed the crypto-resistance of the advanced algorithm to linear and differential cryptanalysis and determined that the speed of cryptographic data processing by the advanced method using the developed encryption function is 1.98 times higher than analogues, and the key generation speed 1.17 times compared to the generators used in particular in the selected prototype.*

Keywords: statistical stability, speed characteristics, hashing function, cryptographic protection, information and communication system.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

На сучасному етапі розвитку хмарних технологій, існує завдання захисту даних, які зберігаються у відповідних інформаційно-комунікаційних системах. Це підтверджується подіями початку 2022 року в України, коли було реалізовано ряд кібератак на хмарні ресурси державних установ. Під час масованої кібератаки, яка почалася у ніч з 13-го на 14 січня 2022 року, постраждали 22 сайти органів державної влади. Шести сайтам було завдано значної шкоди, 70 – відключено за вказівкою Держспецзв'язку та Служби безпеки України [1]. Починаючи з другої половини дня 15 лютого 2022 року спостерігалась потужна DDoS-атака на низку інформаційних ресурсів України. Зокрема, було зафіксовано перебої в роботі веб-сервісів Приватбанку та Ощадбанку. Також атаки зазнали сайти Міністерства оборони та Збройних Сил України [2]. Аналіз останніх подій показав, що хмарні сервіси потребують розроблення нових або удосконалення існуючих механізмів захисту інформації. Одними з таких механізмів є програмні модулі криптографічного захисту даних, у яких необхідно реалізовувати вибір стійких методів шифрування та гешування, а також синхронізацію секретного ключа. У якості зазначених процедур можуть використовуватись відомі криптографічні методи і засоби, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

Аналіз останніх джерел

Сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи [3]. У теперішній час в хмарних сервісах використовуються наступні відомі програмні модулі криптографічного захисту даних: MTProto 1.0 [4] – модуль, який використовується для шифрування повідомлень при передаванні клієнтами Telegram; Signal Protocol [5] – використовується для шифрування миттєвих повідомлень Facebook Messenger; TLS Skype [6] – для миттєвих повідомлень використовується TLS (безпека на рівні транспорту) для шифрування повідомлень між клієнтом Skype та службою чату, коли вони надсилаються безпосередньо між двома клієнтами Skype. Проведений порівняльний аналіз розглянутих модулів захисту інформації у сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). за такими критеріями, як використовувані криптоалгоритми, швидкість роботи (ШР), зручність для користувачів (ЗК) і кросплатформеність (КП), показав, що розглянуті програмні модулі мають низку недоліків і можуть бути удосконалені за рахунок використання сучасних процедур безпеки [16]. Зважаючи на зазначене, в роботі [16] був розроблений удосконалений модуль криптографічного захисту інформації для забезпечення конфіденційності та цілісності даних у сучасних ІКСМ. Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc}. Удосконалений модуль криптографічного захисту інформації, за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ [16]. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа $authKey$. У якості функцій F_{enc} та F_{hash} можуть бути використані зокрема й алгоритми, запропоновані авторами у своїх попередніх роботах [8, 10–12, 16], або інші відомі криптоалгоритми [7, 9, 13–15], стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Областю застосування запропонованих підходів є хмарні системи які описані у [19-20].

Методи дослідження. Основні теоретичні положення роботи отримані з використанням методів теорії захисту інформації.

Об'єктом дослідження є процес забезпечення конфіденційності даних в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій.

Предметом є дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах.

Метою даної роботи є дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій.

Виклад основного матеріалу
Теоретичне обґрунтування удосконалення модуля захисту

З огляду на результати проведеного аналізу, прототипом було обрано розглянутий модуль MTProto Mobile Protocol v.1.0 [4], порівняно з яким було змінено наступне [16]:

1. Змінені вхідні та вихідні дані. На вході приймаються і обробляються наступні дані: повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії S, інформацію про час відправлення і довжину повідомлення ID та порядковий номер повідомлення PD. На виході тільки отримуємо $mHash$ – геш значення DB ($DB = (S, ID, M)$) та $EncP$ – зашифроване повідомлення P [16].

2. Замість використання геш функції SHA-1 введено використання певної криптостійкої геш функції F_{hash}. Слід зауважити, що у якості F_{hash} може бути використана функція гешування, що побудована

на основі одного із методів [7–9, 16].

3. Замість використання блокового шифру AES введено використання функції F_{enc}. Слід зауважити, що у якості F_{enc} може бути використаний певний криптостійкий алгоритм шифрування, побудований на основі блокових, потокових шифрів чи геш функцій тощо [10–12, 16].

4. У якості *authKey*, введено використання заздалегідь узгодженого секретного ключа користувачів, наприклад за допомогою протоколів асиметричної криптографії [16].

Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc}.

Дослідження статистичної стійкості запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах

Розглянемо детальніше опис тестів NIST STS:

1. Частотний (монобітний тест). Суть даного тесту полягає у визначенні співвідношення між нулями і одиницями у всій двійковій послідовності. Мета – з'ясувати, чи дійсне число нулів і одиниць в послідовності приблизно однакові, як це можна було б передбачити в разі достеменний випадковій бінарній послідовності. Тест оцінює, наскільки близька доля одиниць до 0,5. Таким чином, число нулів і одиниць має бути зразкове однаковим. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то дана двійкова послідовність не є істинно випадковою. Інакше, послідовність носить випадковий характер. Варто відзначити, що все подальші тести проводяться за умови, що пройдений даний тест.

2. Частотний блоковий тест. Суть тесту – визначення долі одиниць усередині блоку довжиною m біт. Мета – з'ясувати чи дійсно частота повторення одиниць в блоці довжиною m біт приблизно дорівнює $\frac{m}{2}$, як можна було б передбачити в разі абсолютно ВП. Обчислене в ході тесту значення ймовірності p має бути не менше 0,01. Інакше ($p \prec 0.01$), двійкова послідовність не носить істинно випадковий характер. Якщо прийняти $m = 1$, даний тест переходить в тест № 1 (частотний побітовий тест).

3. Тест на щонайдовшу послідовність одиниць в блоці. У даному тесті визначається найдовший ряд одиниць усередині блоку довжиною m біт. Мета – з'ясувати чи дійсно довжина такого ряду відповідає чеканням довжини найпротяжнішого ряду одиниць в разі абсолютний ВП. Якщо вирахуване в ході тесту значення ймовірності $p \prec 0.01$ вважається, що вихідна послідовність не є випадковою. Інакше, робиться висновок про її випадковість. Слід зауважити, що з припущення про приблизно однакову частоту появи одиниць і нулів (тест № 1) витікає, що такі самі результати даного тесту будуть отримані при розгляді щонайдовшого ряду нулів. Тому виміри можна проводити лише з одиницями.

4-5. Тест на послідовність однакових бітів. Суть полягає в підрахунку повного числа рядів у вихідній послідовності, де під словом «ряд» мається на увазі безперервна підпослідовність однакових бітів. Ряд завдовжки k біт складається з k абсолютно ідентичних бітів, починається і закінчується з біта, що містить протилежне значення. Мета даного тесту – зробити вивід про те, чи дійсна кількість рядів, що складаються з одиниць і нулів з різними довжинами, відповідає їх кількості у ВП. Зокрема, визначається швидко або повільно чергуються одиниці і нулі у вихідній послідовності. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то дана двійкова послідовність не є істинно випадковою. Інакше, вона носить випадковий характер.

6. Тест рангів бінарних матриць. Тут виробляється розрахунок рангів підматриць, що не перетинаються, побудованих з вихідної двійкової послідовності. Метою цього тесту є перевірка на лінійну залежність підрядків фіксованої довжини, складових первинної послідовності. У випадку, якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, робиться вивід про невипадковий характер вхідної послідовності біт. Інакше, вважаємо її абсолютно випадковою. Даний тест так само присутній в пакеті DIEHARD.

7. Спектральний тест. Суть тесту полягає в оцінці висоти піків дискретного перетворення Фур'є вихідній послідовності. Мета – виявлення періодичних властивостей вхідної послідовності, наприклад, близько розташованих один до одного ділянок, що повторюються. Тим самим це явно демонструє відхилення від випадкового характеру досліджуваної послідовності. Ідея полягає в тому, щоб число піків, що перевищують порогове значення в 95 % по амплітуді, було значно більше 5 %. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то дана двійкова послідовність не є абсолютно випадковою. Інакше, вона носить випадковий характер.

8. Тест на збіг шаблонів, що перекриваються. Суть даного тесту полягає в підрахунку кількості заздалегідь визначених шаблонів, знайдених у вихідній послідовності. Як і в тесті № 7 на збіг шаблонів, що не перекриваються, для пошуку конкретних шаблонів довжиною m біт використовується вікно також довжиною m біт. Сам пошук виробляється аналогічним чином. Якщо шаблон не виявлений, вікно зміщується на один біт. Різниця між цим тестом і тестом № 7 полягає лише в тому, що якщо шаблон знайдений, вікно переміщається лише на біт вперед, після чого пошук продовжується далі. Обчислене в ході тесту значення ймовірності p має бути не менше 0,01. Інакше ($p \prec 0.01$), двійкова послідовність не є абсолютно випадковою.

9. Універсальний статистичний тест Маурера. Тут визначається число біт між однаковими шаблонами у вихідній послідовності (міра, що має безпосереднє відношення до довжини стислої послідовності). Мета тесту – з'ясувати чи може дана послідовність бути значно стисла без втрат інформації. У випадку, якщо це можливо зробити, то вона не є істинно випадковою. В ході тесту обчислюється значення ймовірності p. Якщо $p \prec 0.01$, то вважається, що вихідна послідовність не є випадковою. Інакше, робиться вивід про її випадковість.

10. Тест приблизної ентропії. Як і в тесті на періодичність, в даному тесті акцент робиться на підрахунку частоти всіх можливих перекривань шаблонів довжини m біт впродовж вихідної послідовності бітів. Мета тесту – порівняти частоти перекривання двох послідовних блоків вихідної послідовності з довжинами m і $m+1$з частотами перекривання аналогічних блоків в абсолютно ВП. Обчислюване в ході тесту значення ймовірності p має бути не менше 0,01. Інакше ($p \prec 0.01$), двійкова послідовність не є абсолютно випадковою.

11. Тест на довільні відхилення. Суть даного тесту полягає в підрахунку числа циклів, що мають строго k відвідин при довільному обході кумулятивної суми. Довільний обхід кумулятивної суми починається з часткових сум після послідовності (0,1), переведений у відповідну послідовність (-1, +1). Цикл довільного обходу складається з серії кроків одиничної довжини, що здійснюються у випадковому порядку. Крім того такий обхід починається і закінчується на одному і тому ж елементі всередині циклу від аналогічного числа в разі абсолютній випадковій вхідній послідовності. Фактично даний тест є набір, що складається з восьми тестів, що проводяться для кожного з восьми станів циклу: −4, −3, −2, −1 і +1, +2, +3, +4. У кожному такому тесті приймається рішення про міру випадковості вихідної послідовності відповідно до наступного правила: якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то вхідна двійкова послідовність не є абсолютно випадковою. Інакше, вона носить випадковий характер [7].

12. Інший тест на довільні відхилення. У цьому тесті підраховується загальне число відвідин певного стану при довільному обході кумулятивної суми. Метою є визначення відхилень від очікуваного числа відвідин різних станів при довільному обході. Насправді цей тест складається з 18 тестів, що проводяться для кожного стану: −9, −8, …, −1 й +1, +2, …, +9. На кожному етапі робиться вивід про випадковість вхідної послідовності. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то вхідна двійкова послідовність не є абсолютно випадковою. Інакше, вона носить випадковий характер.

13. Тест на періодичність. Даний тест полягає в підрахунку частоти всіх можливих перекривань шаблонів довжини m біт впродовж вихідної послідовності бітів. Метою є визначення чи дійсна кількість появ 2^m шаблонів, що перекриваються, довжиною m біт, приблизне таке ж як в разі абсолютний випадковій вхідній послідовності біт. Остання, як відомо, володіє одноманітністю, тобто кожен шаблон довжиною m біт з'являється в послідовності з однаковою ймовірністю. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то дана двійкова послідовність не є абсолютно випадковою. Інакше, вона носить випадковий характер. Варто відзначити, що при $m = 1$ тест на періодичність переходить в частотний побітовий тест (№ 1).

14. Тест кумулятивних сум. Тест полягає в максимальному відхиленні (від нуля) при довільному обході, визначуваним кумулятивною сумою заданих (-1, +1) цифр в послідовності. Мета даного тесту – визначити чи є кумулятивна сума часткових послідовностей, що виникають у вхідній послідовності, дуже великій або дуже маленькій в порівнянні з очікуваною поведінкою такої суми для абсолютно випадкової вхідної послідовності. Таким чином, кумулятивна сума може розглядатися як як довільний обхід. Для ВП відхилення від довільного обходу мають бути поблизу нуля. Для деяких типів послідовностей, що немає повною мірою випадковими подібні відхилення від нуля при довільному обході будуть досить істотними. Якщо обчислене в ході тесту значення ймовірності $p \prec 0.01$, то вхідна двійкова послідовність не є абсолютно випадковою. Інакше, вона носить випадковий характер [30].

15. Тест на збіг шаблонів, що не перекриваються. У даному тесті підраховується кількість заздалегідь визначених шаблонів, знайдених у вихідній послідовності. Мета – виявити генератори випадкових або псевдовипадкових чисел, що формують дуже часто задані неперіодичні шаблони. Як і в тесті № 8 на збіг шаблонів, що перекриваються, для пошуку конкретних шаблонів довжиною m біт використовується вікно також довжиною m біт. Якщо шаблон не виявлений, вікно зміщується на один біт. Якщо ж шаблон знайдений, вікно переміщається на біт, наступний за знайденим шаблоном, і пошук продовжується далі. Обчислене в ході тесту значення ймовірності p має бути не менше 0,01. Інакше ($p \prec 0.01$), двійкова послідовність не є абсолютно випадковою.

16. Тест на лінійну складність. У основі тесту лежить принцип роботи лінійного регістра зрушення із зворотним зв'язком (англ. Linear Feedback Shift Register, LFSR). Мета – з'ясувати чи є вхідна послідовність досить складною для того, щоб вважатися абсолютно випадковою. Абсолютно ВП характеризуються довгими лінійними регістрами зрушення із зворотним зв'язком. Якщо ж такий регістр дуже короткий, то передбачається, що послідовність не є повною мірою випадковою. В ході тесту обчислюється значення ймовірності p. Якщо $p \prec 0.01$, то вважається, що вихідна послідовність не є випадковою. Інакше, робиться вивід про її випадковість.

Статистичним портретом генератора є матриця розмірністю $m \times q$, де m – кількість двійкових послідовностей, що перевіряються, а q – кількість статистичних тестів, використовуваних для тестування кожної послідовності. Елементи матриці $P_{ij} \in [0,1]$, де $i = \overline{1, m}$ і $j = \overline{1, q}$ є значеннями ймовірності, яка отримана в результаті тестування i-ї послідовності j-м тестом.

1. Згідно з отриманим статистичним портретом визначають долю послідовностей, які пройшли кожен статистичний тест. Для цього задають рівень значущості $\alpha \in [0.001,\ 0.01]$ і виконують підрахунок значень ймовірності, що перевищують встановлений рівень значущості α для кожного з q тестів, тобто визначають коефіцієнт:

$$r_j = \frac{\#\left\{P_{ij} \geq \alpha \middle| i = \overline{1, m}\right\}}{m}$$

В результаті формується вектор коефіцієнтів $\mathbf{R} = \{r_1, r_2, r_q\}$, елементи якого характеризують, у відсотках, проходження послідовності S_i всіх статистичних тестів.

Правило 1. Передбачається, що генератор G пройшов тестування по j-у тесту, якщо значення коефіцієнта r_j знаходиться в межах довірчого інтервалу $[r_{\max}, r_{\min}]$. Кордони довірчого інтервалу визначаються відповідно до вираження:

$$r_{\max(\min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}, \text{ де } \hat{p} = 1 - \alpha.$$

2. Виробляється статистичний аналіз статистичного портрета. Набутих значень ймовірності P_{ij} підкоряються рівноймовірному закону розподілу на інтервалі $[0, 1]$. Для вектора-стовпця статистичного портрета будується гістограма частот F_k попадання значень P_{ij} в кожен з $k = \overline{1, 10}$ підінтервалів, на які розбитий інтервал $[0, 1]$. Рівноймовірність розподілу значень ймовірності P_{ij}, перевіряється з використанням критерію χ^2. Для цього розраховується статистика вигляду:

$$\chi_j^2 = \sum_{k=1}^{10} \frac{\left(F_k - m/10\right)^2}{m/10},$$

яка підкоряється розподілу χ^2 з дев'ятьма мірами свободи.

Правило 2. Передбачається, що генератор G пройшов тестування по j-у тесту, якщо виконується умова $P\left(\chi_j^2\right) > 0.0001$.

3. Передостаннє рішення приймають відповідно до правила: передбачається, що генератор G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для всіх $j = \overline{1, q}$ знаходяться в межах довірчого інтервалу $[r_{\min}, r_{\max}]$ і виконується умова $P\left(\chi_j^2\right) > 0.0001$ для всіх $j = \overline{1, q}$.

Результат тестування (усереднений):

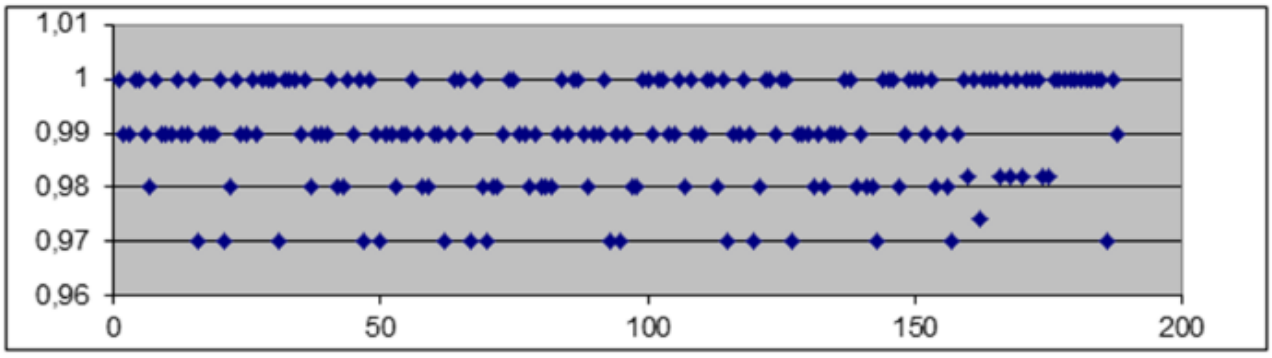

Рис. 1. Статистичний портрет програмної реалізації алгоритму блокового шифрування NRC21 у режимі лічильника Дослідження швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах

Для проведення порівняння швидкостей прототипу (оригіналу алгоритму RC6) та удосконаленого методу перетворення інформації було взято ПЗ симетричного алгоритму шифрування RC6 та створено ПЗ його модифікації.

Таблиця 1

Порівняння швидкості шифрування та дешифрування

№	RC6	NRC21	Генератор RC6	NRC21-Gen
1	16.45 Мб/с	19.38 Мб/с	19.98 Мб/с	22.67 Мб/с
2	6.58 Мб/с	7.75 Мб/с	7.99 Мб/с	9.07 Мб/с
3	21.39 Мб/с	25.19 Мб/с	25.97 Мб/с	29.47 Мб/с
4	10.97 Мб/с	12.92 Мб/с	13.32 Мб/с	15.11 Мб/с
5	24.68 Мб/с	29.07 Мб/с	29.97 Мб/с	34.01 Мб/с

А для проведення порівняльного аналізу швидкостей розробленого генератора криптографічних ключів з генератором ключів, що використовується в алгоритмі RC6 та лінійно конгруентним генератором було взято ПЗ зазначених генераторів та створено ПЗ розробленого генератора криптографічних ключів (табл. 1).

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ управління технологічними процесами. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа *authKey*. У якості функцій F_{enc} та F_{hash} можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведено експериментальне дослідження, що підтвердило криптостійкість удосконаленого алгоритму до лінійного та диференціального криптоаналізу та дозволило визначити, що швидкість криптографічної обробки даних удосконаленим методом з використанням розробленої функції шифрування є у 1,98 разів вищою у порівнянні з аналогами, а швидкість генерування ключів є вищою відповідно у 1,17 разів в порівнянні з генераторами, що використовуються зокрема в обраному прототипі.

Література

1. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku

2. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

3. R. Oppliger, Cryptography 101: *From Theory to Practice,* Artech, 2021.

4. Job J., Naresh V. and K. Chandrasekaran, "A modified secure version of the Telegram protocol (MTProto)", 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2015, pp. 1-6

5. Dion van Dam, Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol, 21 August 2019, 61 p.

6. TLS and SRTP for Skype Connect Technical Datasheet, 2011, 8 p.

7. Q. Wu, "A Chaos-Based Hash Function", 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2015, pp. 1-4,

8. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, *Advances in Intelligent Systems and Computing*, Vol. 902, pp. 561-569, 2020.

9. K. Rajeshwaran and K. Anil Kumar, "Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function", *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1-6

10. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch, *Communications in Computer and Information Science*, Vol. 1486, pp. 185-193, 2021.

11. Gnatyuk S., Iavich M., Kinzeryavyy V., Okhrimenko T., Burmak Y., Goncharenko I. Improved secure stream cipher for cloud computing, *CEUR Workshop Proceedings*, Vol. 2732, pp. 183-197, 2020.

12. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, *Advances in Intelligent Systems and Computing*, Vol. 1126, pp. 93-104, 2020.

13. A. Kuznetsov, I. Horkovenko, O. Maliy, N. Goncharov, T. Kuznetsova and N. Kovalenko, "Non-Binary Cryptographic Functions for Symmetric Ciphers", 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 567-572, doi: 10.1109/PICST51311.2020.9467982.

14. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA

Cryptosystems", *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

15. T. R. Lee, J. S. Teh, N. Jamil, J. L. S. Yan and J. Chen, "Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes", in *IEEE Access*, vol. 9, pp. 134052-134064, 2021, doi: 10.1109/ACCESS.2021.3116468.

16. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Бурмак Ю.А., Оспанова Д.М. «Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах». *Кібербезпека: освіта, наука, техніка*. № 2(14). С. 176-185. 2021.

17. Смірнова Т.В., Поліщук Л.І., Смірнов О.А., Буравченко К.О., Макевнін А.О. «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.

18. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дреєв О.М. «Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей», *Центральноукраїнський науковий вісник. Технічні науки.* № 1(32). с. 184-194, 2019.

19. Смірнова, Т.В., Смірнов, С.А., Минайленко, Р.М., Доренський, О.П., Сисоєнко С.В. «Хмарна автоматизована система інтелектуальної підтримки прийняття рішень для технологічних процесів». *Вісник Черкаського державного технологічного університету. Технічні науки.* № 4, 2020, С. 84-92.

20. Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., Смірнов О.А. «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95.

References

1. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku

2. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

3. R. Oppliger, Cryptography 101: From Theory to Practice, Artech, 2021.

4. Job J, Naresh V and K. Chandrasekaran, "A modified secure version of the Telegram protocol (MTProto)", 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2015, pp. 1-6,

5. Dion van Dam, Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol, 21 August 2019, 61 p.

6. TLS and SRTP for Skype Connect Technical Datasheet, 2011, 8 p.

7. Q. Wu, "A Chaos-Based Hash Function", 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2015, pp. 1-4,

8. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, Advances in Intelligent Systems and Computing, Vol. 902, pp. 561-569, 2020.

9. K. Rajeshwaran and K. Anil Kumar, "Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function", 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, pp. 1-6,

10. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch, Communications in Computer and Information Science, Vol. 1486, pp. 185-193, 2021.

11. Gnatyuk S., Iavich M., Kinzeryavyy V., Okhrimenko T., Burmak Y., Goncharenko I. Improved secure stream cipher for cloud computing, CEUR Workshop Proceedings, Vol. 2732, pp. 183-197, 2020.

12. Gnatyuk S., Akhmetov B., Kozlovskyi V., Kinzeryavyy V., Aleksander M., Prysiazhnyi D. New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, Vol. 1126, pp. 93-104, 2020.

13. A. Kuznetsov, I. Horkovenko, O. Maliy, N. Goncharov, T. Kuznetsova and N. Kovalenko, "Non-Binary Cryptographic Functions for Symmetric Ciphers", 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 567-572, doi: 10.1109/PICST51311.2020.9467982.

14. E. Jintcharadze and M. Iavich, "Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems", 2020 IEEE East-West Design & Test Symposium (EWDTS), 2020, pp. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.

15. T. R. Lee, J. S. Teh, N. Jamil, J. L. S. Yan and J. Chen, "Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes", in IEEE Access, vol. 9, pp. 134052-134064, 2021, doi: 10.1109/ACCESS.2021.3116468.

16. Smirnova T.V., Gnatiuk S.O., Berdybaev R.S., Burmak Y.A., Ospanova D.M., «Udoskonalenyi modul kryptohrafichnoho zakhystu informatsii v suchasnykh informatsiino-komunikatsiinykh systemakh ta merezhakh» [Advanced module of cryptographic protection of information in modern information and communication systems and networks]. Cybersecurity: education, science, technology. № 2 (14). Pp. 176-185. 2021

17. Smirnova T.V., Polishchuk L.I., Smirnov O.A., Buravchenko K.O., Makevnin A.O., «Doslidzhennia khmarnykh tekhnolohii yak servisiv» [Research of cloud technologies as services], Cybersecurity: education, science, technology. № 3 (7). Pp. 43-62. 2020

18. Smirnova T.V., Solovykh E.K., Smirnov O.A., Dreev O.M., «Pobudova khmarnykh informatsiinykh tekhnolohii optymizatsii tekhnolohichnoho protsesu vidnovlennia ta zmitsnennia poverkhon detalei»[Construction of cloud information technologies to optimize the technological process of restoration and strengthening of surfaces of parts], Central Ukrainian Scientific Bulletin. Technical sciences. № 1 (32). pp. 184-194, 2019

19. Smirnova, T.V., Smirnov, S.A., Minailenko, R.M., Dorensky, O.P., Sysoenko S.V. «Khmarna avtomatyzovana systema intelektualnoi pidtrymky pryiniattia rishen dlia tekhnolohichnykh protsesiv». [Cloud automated system of intelligent decision support for technological processes]. Bulletin of Cherkasy State Technological University. Technical sciences. №4, 2020, pp. 84-92.

20. Smirnova T.V., Buravchenko K.O., Kravchenko S.S., Gorbov V.O., Smirnov O.A. «Khmarna systema pidtrymky pryiniattia rishen tekhnolohichnoho protsesu vidnovlennia poverkhon konstruktsii i detalei mashyn». [Cloud system to support decision-making of the technological process of restoration of surfaces of structures and machine parts]. Modern information systems. 2021. T. 5, № 4. S. 79-95.