УДК 003.26:004.056.5
DOI https://doi.org/10.32689/maup.it.2023.5.8

Володимир БРОДКЕВИЧ
кандидат економічних наук, доцент кафедри комп'ютерно-інформаційних систем і технологій Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, індекс 03039 (v.brodkevych@gmail.com)
ORCID: 0000-0003-4282-8888

Дарина ЯРЕМЕНКО
викладач кафедри комп'ютерних наук та інтелектуальних систем Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, індекс 03039 (dashayaremenko17@gmail.com)
ORCID: 0000-0002-6294-9698

Віталій КИРИЧЕНКО
аспірант кафедри комп'ютерно-інформаційних систем і технологій Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, індекс 03039 (vp_kirichenko@ukr.net)
ORCID: 0009-0005-5411-4315

Андрій ШЛАПАК
аспірант кафедри комп'ютерно-інформаційних систем і технологій Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, індекс 03039 (Andreii.shlapak@gmail.com)
ORCID: 0009-0001-7563-4871

Олег ТИЩЕНКО
аспірант кафедри комп'ютерно-інформаційних систем і технологій Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, індекс 03039 (0987651234um@gmail.com)
ORCID: 0009-0001-2763-579X

Volodymyr BRODKEVYCH
Candidate of Economic Sciences, Associate Professor at the Department of Computer Information Systems and Technologies of the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine postal code 03039 (v.brodkevych @gmail.com)

Daryna YAREMENKO
Lecturer at the Department of Computer Science and Intelligent Systems of the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine postal code 03039 (dashayaremenko17@gmail.com)

Vitalii KYRYCHENKO
Postgraduate Student at the Department of Computer Information Systems and Technologies of the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine postal code 03039 (vp_kirichenko@ukr.net)

Andrii SHLAPAK
Postgraduate Student at the Department of Computer Information Systems and Technologies of the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine postal code 03039 (Andreii.shlapak@gmail.com)

Oleh TYSHCHENKO
Postgraduate Student at the Department of Computer Information Systems and Technologies of the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine postal code 03039 (0987651234um@gmail.com)

Бібліографічний опис статті: Бродкевич, В., Яременко, Д., Кириченко, В., Шлапак, А., Тищенко О. (2023). Застосування шифрування даних в управлінській діяльності. *Інформаційні технології та суспільство,* 5 (11), 60–66. DOI: https://doi.org/10.32689/maup.it.2023.5.8

Bibliographic description of the article: Brodrevych, V., Yaremenko, D., Kyrychenko, V., Shlapak, A., Tyshchenko, O. (2023). Zastosuvannia shyfruvannia danykh v upravlinskii diialnosti [Application of data encryption in administrative activities]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society,* 5 (11), 60–66. DOI: https://doi.org/10.32689/maup.it.2023.5.8

ЗАСТОСУВАННЯ ШИФРУВАННЯ ДАНИХ В УПРАВЛІНСЬКІЙ ДІЯЛЬНОСТІ

Анотація. *У сучасному цифровому світі, де велика частина бізнес-операцій і обміну даними відбувається в електронному форматі, шифрування стає незамінним інструментом для забезпечення безпеки. Дана стаття присвячена опису розробленого прикладного програмного забезпечення, що реалізує алгоритми шифрування даних. Програмний застосунок може бути використаний в управлінській діяльності для забезпечення достатнього рівня захисту даних, враховуючи потенційні загрози. До чутливих даних компанії, що потребують особливої уваги з точки зору безпеки відносяться наступні: комерційна таємниця, фінансова інформація, внутрішня кореспонденція, персональні дані співробітників й клієнтів тощо. Шифрування цих типів даних дозволяє компаніям захистити свою комерційну інформацію, знизити ризик фінансових та репутаційних втрат. При розробці програмного забезпечення використовувалися алгоритми ChaCha20 і Poly1305 в декілька ключових етапів. Спочатку реалізовано основні функції, такі як QuarterRound і ChaChaBlock, які виконують перетворення стану ChaCha20. Далі створено механізм шифрування відкритого тексту, розбивши його на блоки і використовуючи XOR для обробки кожного блоку згенерованим потоком ключів. Крім того, імплементовано функцію аутентифікації повідомлень Poly1305, що генерує тег для перевірки цілісності даних. Завершальним етапом було інтегрування обох частин системи – шифрування та аутентифікації, щоб забезпечити конфіденційність та цілісність переданих даних. Також проведено тестування розробленого програмного забезпечення, що показало коректність його роботи. Розроблений застосунок легко інтегрується в майже будь-яку IT-інфраструктуру компанії, може працювати в реальному часі для шифрування внутрішньої кореспонденції або повідомлені по мережі компанії. Завдяки відкритому коду, програмне забезпечення може буде вдосконалено під умови замовника (наприклад для шифрування документів в різних форматах для довготривалого збереження та/або переказу по відкритому каналу зв'язку).*

Ключові слова: *прикладне програмне забезпечення, комерційна таємниця, шифрування даних, цілісність та автентичність.*

APPLICATION OF DATA ENCRYPTION IN MANAGEMENT ACTIVITIES

Abstract*. In today's digital world, where a significant portion of business operations and data exchange takes place in electronic format, encryption becomes an indispensable tool for ensuring security. This article is dedicated to the description of the developed application software that implements data encryption algorithms. The software application can be used in managerial activities to provide an adequate level of data protection, considering potential threats. Sensitive company data that require special attention in terms of security include the following: trade secrets, financial information, internal correspondence, as well as personal data of employees and clients, etc. Encrypting these types of data allows companies to protect their commercial information, reduce the risk of financial and reputational losses. In developing the software, the ChaCha20 and Poly1305 algorithms were used at several key stages. Initially, the core functions, such as QuarterRound and ChaChaBlock, which perform the transformation of the ChaCha20 state, were implemented. Then, a mechanism for encrypting plain text was created by dividing it into blocks and using XOR to process each block with the generated key stream. In addition, the Poly1305 message authentication function, which generates a tag for verifying data integrity, was implemented. The final stage was the integration of both parts of the system – encryption and authentication, to ensure the confidentiality and integrity of the transmitted data. Testing of the developed software was also conducted, demonstrating its correct operation. The developed application is easily integrated into almost any company's IT infrastructure, can operate in real-time for encrypting internal correspondence or company network messages. Thanks to the open-source code, the software can be refined under customer conditions (for example, for encrypting documents in various formats for long-term storage and/or transmission over an open communication channel).*

Key words**:** *software, encryptions algorytms, trade secrets, finance information, personal data.*

На сьогодні у сфері управлінської діяльності існує декілька різновидів «чутливих» даних, що потребують ретельного збереження та/або переказу. До таких видів можна віднести:

– персональні дані співробітників (ім'я, адреса, номер соціального страхування, банківські реквізити, медична інформація тощо);

– фінансова інформація (банківські рахунки компанії, звіти про прибутки та збитки, інвестиційні стратегії, аудиторські висновки тощо);

– внутрішня кореспонденція та документація (електронні листи, звіти, протоколи зборів, внутрішні настанови та політики);

– дані про клієнтів (контактна інформація, історія покупок, персональні уподобання та потреби);

– договори та угоди (контракти з партнерами, постачальниками, клієнтами, умови ліцензійних угод);

– дані про продукцію та послуги (описи, технічні характеристики, ціни, плани виробництва).

Особливу увагу також слід приділяти комерційній таємниці. Комерційна таємниця є ключовим активом для будь-якої організації, оскільки вона включає в себе відомості, що мають комерційну вартість через те, що вони невідомі широкому колу осіб і перед якими їх власник здійснює заходи щодо збереження конфіденційності. Це можуть бути формули, рецепти, проектні документи, стратегії розвитку, бази даних клієнтів, виробничі секрети, унікальні рецептури, технологічні процеси, маркетингові

стратегії та будь-яка інша інформація, яка допомагає компанії зберегти та посилити свої конкурентні переваги.

Захист комерційної таємниці має критичне значення. Наведемо декілька аргументів щодо цього ствердження. По перше це конкурентна перевага на ринку. Унікальна інформація, яка не доступна конкурентам, може надавати значну перевагу, дозволяючи пропонувати унікальні продукти чи послуги.

Другим аспектом може бути фінансова стабільність. Інформація, що становить комерційну таємницю, може впливати на доходи та рентабельність компанії. Її втрата або несанкціонований доступ може призвести до фінансових збитків. Також слід відмітити інвестиції акціонерів та подальший розвиток компанії. Компанії, що інвестують у дослідження та розробку, для захисту своїх інвестицій потребують гарантій того, що результати цих діяльностей залишаться винятково у їх розпорядженні.

Також слід відмітити законодавчі вимоги. В багатьох юрисдикціях існують законодавчі акти, що зобов'язують компанії захищати персональні дані клієнтів та іншу конфіденційну інформацію. Отже, задача захисту даних в управлінської діяльності є актуальною. Сучасні методи захисту повинні бути комплексними й охоплювати як технічні, так і організаційні заходи. До них ми будемо відносити наступні:

Шифрування даних. Використання сучасних методів шифрування для захисту електронних документів та баз даних забезпечує, що інформація залишається недоступною для несанкціонованих осіб.

- Контроль доступу. Обмеження доступу до інформації через фізичні та електронні системи контролю доступу дозволяє забезпечити, що тільки уповноважені особи мають доступ до комерційних таємниць.
- Юридичні заходи. Використання конфіденційних угод (NDA), трудових контрактів та інших юридичних інструментів допомагає захистити інформацію на законодавчому рівні.
- Фізична безпека. Захист фізичних носіїв інформації та важливих об'єктів компанії, таких як офіси, виробничі площі та лабораторії, є необхідним елементом загальної стратегії безпеки.

Дана стаття пропонує до уваги опис програмного рішення алгоритму шифрування даних. Після проведеного огляду сучасних алгоритмів шифрування [1, с. 48-51] було обрано шифр Шифр ChaCha20. Розглянемо його детальніше.

Шифр ChaCha20 – це високошвидкісний потіківий шифр, який був спочатку описаний у документі [2, с. 78-81]. Цей шифр є значно швидшим, ніж AES [3, с. 21] у програмних реалізаціях, що робить його близько втричі швидшим на платформах, де відсутнє спеціалізоване обладнання AES. Крім того, ChaCha20 не чутливий до атак з урахуванням часу. Щодо практичного застосування – ChaCha20 широко використовується в сучасних криптографічних протоколах, таких як TLS, SSH, IPsec [2, с. 6] та інші, як альтернатива AES.

Для досягнення нашої мети будемо імплементувати функцію аутентифікації повідомлень Poly1305, що генерує тег для перевірки цілісності даних. Під час цього етапу будемо використовувати бібліотеку NACL для створення тега Poly1305.

Аутентифікатор Poly1305 – це високошвидкісний аутентифікатор повідомлень, який використовується для перевірки цілісності та автентифікації повідомлень [4, с. 2]. Його реалізація також досить проста та не вимагає спеціальних обчислювальних ресурсів. Poly1305 часто використовується разом з різними шифрами для забезпечення конфіденційності та цілісності даних, зокрема в AEAD конструкціях.

Розглянемо конструкцію CHACHA20-POLY1305 AEAD. Це аутентифікована шифрувальна конструкція з асоційованими даними (AEAD), яка комбінує шифр ChaCha20 і аутентифікатор Poly1305 для забезпечення конфіденційності, цілісності та автентифікації повідомлень та їх асоційованих даних. Ця конструкція широко використовується в сучасних протоколах безпеки, наприклад, таких як TLS 1.3, з метою захисту комунікацій в мережах Інтернету.

Розглянемо більш детально роботу алгоритму. Алгоритм ChaCha20 використовує функцію блока для перетворення стану шляхом виконання кількох чвертей обертання.

Вхідними параметрами алгоритму є:

– 256-бітний ключ, який розглядається як конкатенація восьми 32-бітних малих ендіанів;

– 96-бітний нонс, який розглядається як конкатенація трьох 32-бітних малих ендіанів;

– 32-бітний параметр кількості блоків, який розглядається як 32-бітний малий ендіан.

Вихідним значенням алгоритму є 64 випадкових байтів.

Початковий стан ChaCha20 ініціалізується наступним чином:

– Перші чотири слова (0-3) є константами: 0x61707865, 0x3320646e, 0x79622d32, 0x6b206574.

– Наступні вісім слів (4-11) беруться з 256-бітного ключа, читаючи байти в малих ендіанів, в 4-байтових чанках.

– Слово 12 є лічильником блоків. Оскільки кожен блок має розмір 64 байти, 32-бітне слово достатньо для 256 гігабайтів даних.

– Слова 13-15 є нонсом, який МАЄ не повторюватися для одного ключа. 13-те слово є першими 32 бітами вхідного нонса, взятими як малий ендіан, тоді як 15-те слово є останніми 32 бітами.

Алгоритм ChaCha20, як видно з назви, складається з 20 раундів, які чергуються між «колонковими раундами» та «діагональними раундами». Кожен раунд складається з чотирьох чвертей обертання, і вони виконуються наступним чином. Чверті обертання 1-4 є частиною «колонкового» раунду, тоді як 5-8 є частиною «діагонального» раунду.

На кінці 20 раундів (або 10 ітерацій вищезазначеного списку) ми додаємо початкові вхідні слова до вихідних слів і серіалізуємо результат, впорядкувавши слова одне за одним в малих ендіанах.

Poly1305 – це одноразовий аутентифікатор, розроблений D. J. Bernstein [4, с. 3]. Poly1305 приймає 32-байтний одноразовий ключ і повідомлення, і генерує 16-байтний тег. Цей тег ми будемо використовувати для аутентифікації повідомлення. Poly1305 має назву «Код аутентифікації повідомлень Poly1305-AES", і там функція MAC вимагає 128-бітний ключ AES, 128-бітний «додатковий ключ» і 128-бітний (не секретний) nonce. Алгорим AES використовується там для шифрування nonce, щоб отримати унікальний (і секретний) 128-бітний рядок. При необхідності можна замінити AES на довільну ключову функцію з довільним набором nonce до 16-байтних рядків [5, с. 20].

Незалежно від того, як створюється ключ, ключ розділяється на дві частини, які називаються "r" і "s". Пара (r, s) повинна бути унікальною і НЕПРЕДСКАЗУЄМОЮ для кожного виклику (тому вона спочатку отримується шифруванням nonce), в той час як "r" МОЖЕ бути сталим, але потребує змін, перш ніж використовуватися. ("r" трактується як 16-октетне число little-endian):

– r[3], r[7], r[11] і r[15] повинні мати свої верхні чотири біти встановлені в нуль (бути меншими за 16);

– r[4], r[8] і r[12] повинні мати свої нижні два біти встановлені в нуль (бути кратними 4).

Вхідними параметрами для Poly1305 є:

– 256-бітний одноразовий ключ;

– Повідомлення довільної довжини;

Вихідне значення – це 128-бітний тег.

Спочатку значення "r" стискається.

Далі, встановлюється постійне просте число "P", яке дорівнює 2^130-5: 3ffffffffffffffffffffffffffffffffb. Також встановлюється змінну "accumulator" на нуль.

Після цього повідомлення розділяється на блоки по 16 байт. Останній може бути коротшим:

– Читаємо блок як число little-endian.

– Додаємо один біт поза числом октетів. Для блоку з 16 байт це еквівалентно додаванню 2^128 до числа. Для коротшого блоку це може бути 2^120, 2^112 або будь-яка ступінь двійки, яка рівномірно ділиться на 8, аж до 2^8.

– Якщо блок не має довжини 17 байтів (останній блок), заповнюємо його нулями. Це не має значення, якщо ми трактуємо блоки як числа.

– Додаємо це число до аккумулятора.

– Помножуємо на "r".

– Встановлюємо аккумулятор на результат modulo p. Загалом: Acc = ((Acc + block) * r) % p.

Нарешті, значення секретного ключа "s" додається до аккумулятора, а 128 менш значущих бітів серіалізуються у порядку little-endian для формування тегу.

Далі розглянемо опис програмного забезпечення.

При розробці програмного забезпечення для шифрування даних управлінської діяльності, спочатку було реалізовано функцію QuarterRound. Ця функція виконує одну ітерацію четвертого обертання в алгоритмі ChaCha20. Потім виконано реалізацію функції ChaChaBlock, яка використовує кілька ітерацій QuarterRound для перетворення стану ChaCha.

Ця функція приймає ключ, nonce та лічильник блоків як вхідні параметри і генерує 64 байти випадково виглядаючих даних.

Наступним кроком стала реалізація функції для шифрування відкритого тексту. Вхідний текст було розбито на блоки і застосована операція XOR зі згенерованим потоком ключів. Після успішного шифрування знадобилось також забезпечити аутентифікацію повідомлення.

Для цього було використано бібліотеку NACL для створення тега Poly1305. Під час шифрування згенерований 32-бітний ключ та зашифрований текст передавався в функцію Poly1305, щоб згенерувати тег. Варто зазначити, що під час розшифрування ця функція приймала «відкритий текст», який насправді є зашифрований, аби перевірити, чи не був він змінений під час транспортування.

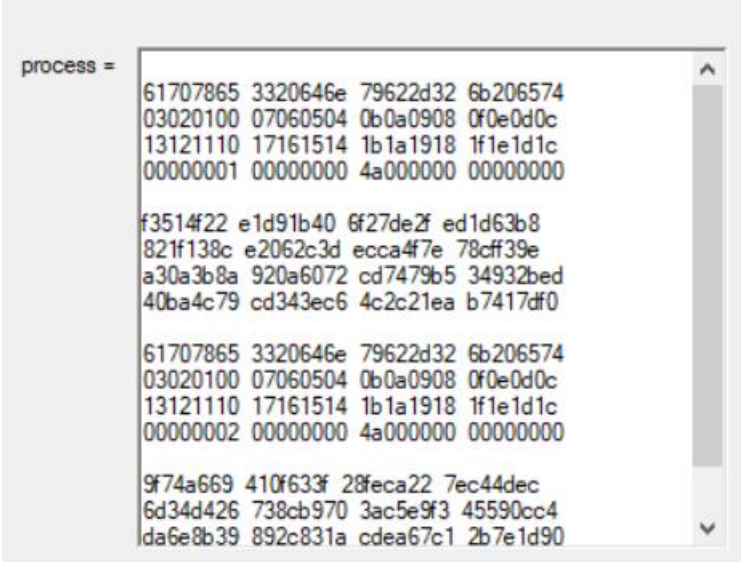

Рис. 1. Вхідні блоки в ChaCha20Block та після проходу 20 раундів

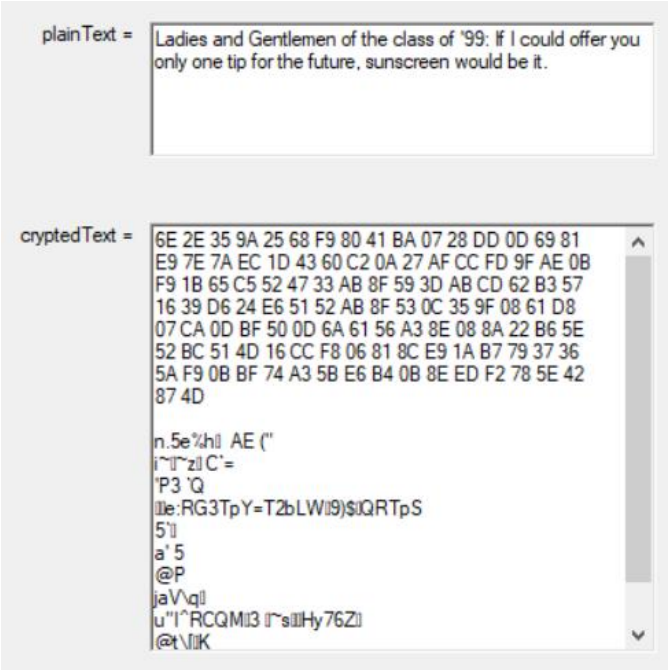

Рис. 2. Відкритий текст та зашифрований

Висновки

1. Шифрування цих типів даних дозволяє компаніям захистити свою комерційну інформацію, знизити ризик фінансових та репутаційних втрат. У сучасному цифровому світі, де велика частина бізнес-операцій і обміну даними відбувається в електронному форматі, шифрування стає незамінним інструментом для забезпечення безпеки.

2. Розроблено прикладне програмне забезпечення для шифрування конфеденційної інформації для управлінської діяльності. Проведено його тестування, показано коректність та продуктивність роботи алгориитмів.

3. Дане програмне забезпечення дозволяє забезпечити достатній рівень захисту даних, враховуючи потенційні загрози. Сумісне з ІТ-інфраструктурою будь-якої компанії та може бути змінено під потреби замовника завдяки відкритому коду.

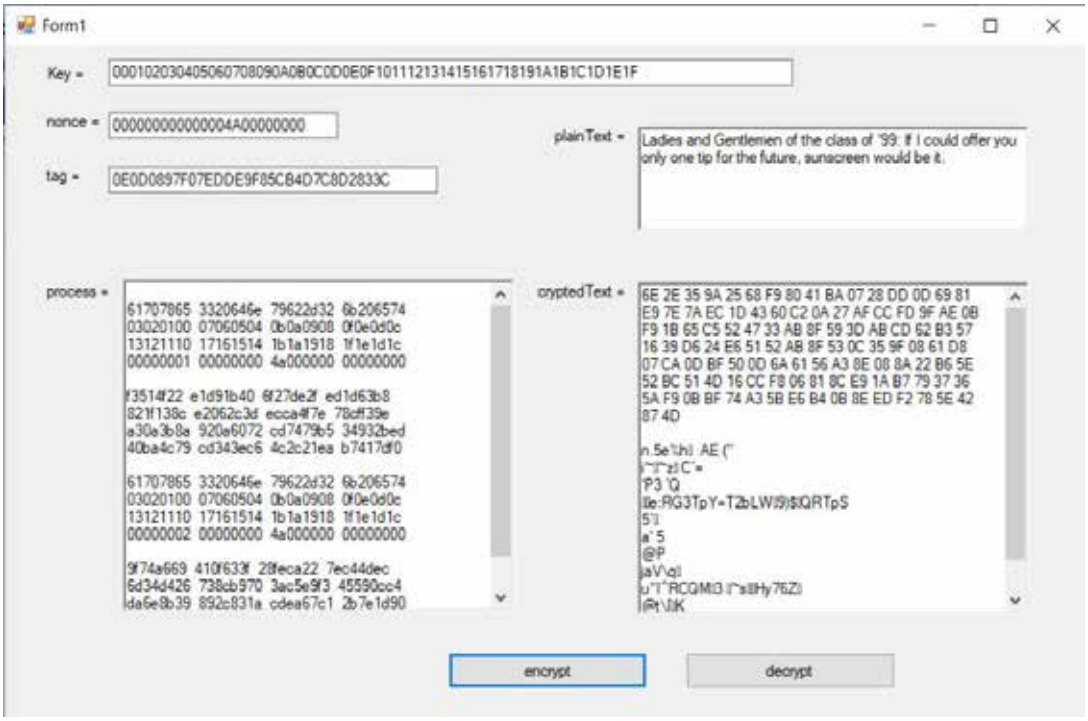

Рис. 3. Шифрування тексту

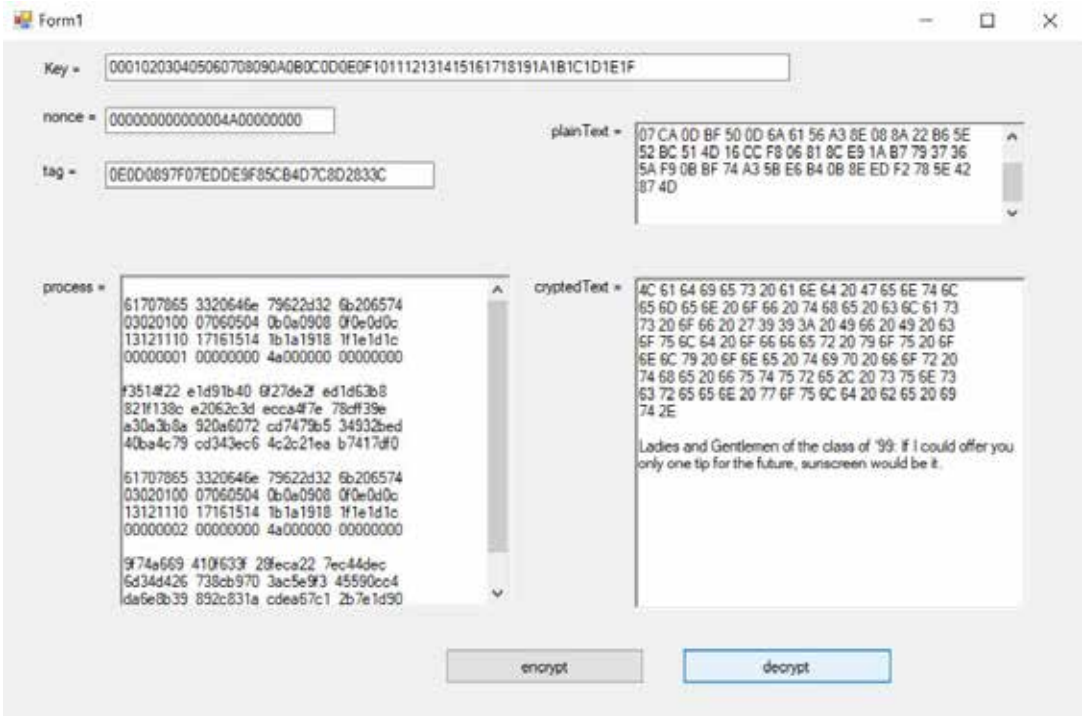

Рис. 4. Розшифрування тексту, перевірка тегу

Під час розробки програми для шифрування і аутентифікації повідомлень з використанням алгоритмів ChaCha20 і Poly1305 я вивчила та реалізувала кілька ключових етапів. Спочатку я розробила основні функції, такі як QuarterRound і ChaChaBlock, які виконують перетворення стану ChaCha20. Далі я створила механізм шифрування відкритого тексту, розбивши його на блоки і використовуючи XOR для обробки кожного блоку згенерованим потоком ключів.

Список використаних джерел:

1. Горбенко І. Д. Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. Харків: Форт, 2013. 80.
2. Совин Я. Р., Хома В. В., Отенко В. І., Порівняння AEAD-алгоритмів для вбудованих систем інтернету речей. 2019. с. 76-91. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2020/feb/21055/var1ksm-19-78-93.pdf
3. AES Encrypter/Decrypter [Електронний ресурс]: ECE 5760: Final Project / A. Laxminarayana, A. Ravani, M. Venkatraman. URL: http://people.ece.cornell.edu/land/courses/ece5760/FinalProjects/s2015/ar856/ECE560webpage/ECE5760%20webpage/webpage_file s.html
4. Bernstein, D.J.: Stronger security bounds for wegman-carter-shoup authenticators. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 164–180. Springer, Heidelberg. 2005. http://cr.yp.to/papers.html#securitywcs, ID2d603727f69542f30f7da2832240c1ad
5. Nir Y. ChaCha20 and Poly1305 for IETF Protocols [Електронний ресурс] / Y. Nir, A. Langley // Google, Inc. 2018.

References:

1. Horbenko I. D. (2013). Applied cryptology: Theory. Practice. Application / I. D. Horbenko, Yu. I. Horbenko. Kharkiv: Fort. 880.
2. Sovin Y. R., Khoma V. V., Otenko V. I. (2019). Comparison of AEAD algorithms for embedded systems of the Internet of Things. pp. 76-91. Retrieved from https://science.lpnu.ua/sites/default/files/journal-paper/2020/feb/21055/var1ksm-19-78-93.pdf
3. AES Encrypter/Decrypter [Electronic resource]: ECE 5760: Final Project / A. Laxminarayana, A. Ravani, M. Venkatraman. Retrieved from http://people.ece.cornell.edu/land/courses/ece5760/FinalProjects/s2015/ar856/ECE560webpage/ ECE5760%20webpage /webpage_file s.html
4. Bernstein, D.J. (2005). Stronger security bounds for wegman-carter-shop authenticators. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 164–180. Springer, Heidelberg. Retrieved from http://cr.yp.to/papers.html#securitywcs,ID2d603727f69542f30f7da2832240c1ad
5. Nir Y. (2018). ChaCha20 and Poly1305 for IETF Protocols [Electronic resource] / Y. Nir, A. Langley // Google, Inc.