НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

References:

1. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), tyab005.
2. Stallings, W. Cryptography and Network Security - Principles and Practice.
3. I F. Volynets-Velikorodov and M. S. Klimash. Prospects for the Application of Many-Valued Logic Functions in Cryptography Proceedings of the 2018 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD).

Ключові слова: кібербезпека, криптографія, багатозначна логіка.
Keywords: cybersecurity, cryptography, many-valued logic.

МЕТОДИ ТА РИЗИКИ ПОБУДОВИ СИСТЕМ З END-TO-END ШИФРУВАННЯМ

Вінковська Ірина

Національний університет «Одеська політехніка»,
старший викладач кафедри кібербезпеки та програмного забезпечення

Чебаненко Олег

Національний університет «Одеська політехніка»,
студент кафедри кібербезпеки та програмного забезпечення

Вступ. Сучасні інформаційні технології забезпечують швидкий обмін даними між користувачами через різноманітні месенджери (Telegram, WhatsApp, Signal тощо). Проте зростання кількості кіберзагроз робить актуальною проблему забезпечення конфіденційності та цілісності повідомлень. Більшість популярних месенджерів використовують власні протоколи шифрування, але їхній вихідний код або архітектура не завжди відкриті для аудиту, що створює ризики втрати контролю над безпекою даних.

У зв'язку з цим постає завдання створення відкритих програмних рішень, які реалізують принцип end-to-end шифрування (E2EE) – коли лише відправник і отримувач мають доступ до змісту повідомлень, а сервер виконує лише роль транспортного посередника.

Мета: Проаналізувати сучасні підходи до реалізації end-to-end шифрування в месенджерах та визначити напрями створення програмного застосунку, який забезпечить конфіденційність, цілісність і автентичність повідомлень під час обміну даними між користувачами.

Проблематика захищеного обміну повідомленнями

Передача даних у мережах часто супроводжується ризиками несанкціонованого доступу, підміни або перехоплення повідомлень.

Уразливими є системи, що не застосовують повноцінного шифрування або використовують слабкі алгоритми. Проблемою також є централізоване зберігання ключів на сервері, що створює можливість їх компрометації.

Багато месенджерів не мають прозорих механізмів обміну ключами, що знижує рівень довіри користувачів і не гарантує повної конфіденційності даних. Тому, створення незалежної клієнтської системи шифруванням є важливою передумовою для підвищення рівня безпеки комунікацій [1].

Методи криптографічного захисту

Основою безпечного обміну даними є асиметричне шифрування, де кожен користувач має пару ключів – відкритий і закритий. У межах дослідження розглядаються алгоритми RSA та ElGamal, які дозволяють здійснювати безпечну передачу даних без необхідності обміну секретними ключами.

Алгоритм RSA ґрунтується на складності факторизації великих чисел. Для роботи генеруються два великі прости числа, на основі яких формується пара ключів: відкритий для шифрування, закритий – для розшифрування.

Алгоритм ElGamal базується на складності обчислення дискретного логарифма, і який створює унікальний шифр текст при кожному шифрування одного й того ж повідомлення [2].

Для забезпечення цілісності даних буде використовуватись криптографічна хеш-функція SHA-256, що перетворює повідомлення на фіксований 256-бітний хеш.

Автентифікація користувачів та підтвердження походження даних забезпечуватимуться за допомогою цифрових підписів, які формуються шляхом шифрування хешу повідомлення закритим ключем відправника [3].

Поєднання асиметричного шифрування (RSA та ElGamal), хешування (SHA-256) та цифрових підписів забезпечить комплексний, багаторівневий захист повідомлень і повну відповідність принципу end-to-end шифрування.

Аналіз проблем та ризиків при побудові месенджера end-to-end шифрування

Під час створення месенджера з end-to-end шифруванням однією з основних проблем є забезпечення захищеного обміну відкритими ключами. У разі їх підміни можливі атаки типу «людина посередині», що дозволяє зловмиснику читати або змінювати повідомлення. Додатковим ризиком є компрометація приватного ключа на пристрої користувача, що відкриває доступ до всієї історії переписки.

Важливою загрозою залишається верифікація автентичності користувачів: навіть при коректній криптографічній реалізації система може бути вразливою до соціальної інженерії або підроблених ключів. Уразливість також виникає під час зберігання локальних даних – зараження пристрою шкідливим ПЗ може призвести до витоку інформації до її шифрування.

Технічні ризики пов'язані з керування ключами та сесіями, неправильним оновленням криптографічного матеріалу та відсутністю механізмів forward secrecy. Навіть за відсутності доступу до відкритих даних компрометація серверної інфраструктури може вплинути на доставку повідомлень і цілісність ключів. Тому побудова безпечного месенджера потребує комплексного підходу, що враховує криптографічні, мережеві та користувацькі ризики.

Висновок. Розробка месенджера з end-to-end шифруванням є актуальним завданням кібербезпеки для захисту даних. Ефективна реалізація E2EE вимагає надійних криптоалгоритмів, безпечного обміну ключами, захисту клієнтських пристроїв та перевірки належної автентифікації. Поєднання RSA, ElGamal, SHA-256 та цифрових підписів створює багаторівневий захист від сучасних загроз. У планах – створення програмного застосунку для практичної демонстрації та підтвердження ефективності цих методів.

Перелік використаних джерел:

1. Наскрізне шифрування: що це таке та як працює. – URL: https://root-nation.com/ua/articles-ua/tech-ua/ua-end-to-end-encryption/
2. Яремчук Ю.Є., Салієва О.В., Бондаренко І.О. Основи криптографічного захисту інформації. – URL: https://pdf.lib.vntu.edu.ua/books/2024/Yaremchuk_2024_139.pdf
3. Що таке криптографія у блокчейні. 2025. – URL: https://www.web3.org.ua/shcho-take-kryptohrafiia-u-blokchejni/

Ключові слова: end-to-end шифрування, RSA, ElGamal, SHA-256, цифровий підпис.
Key words: end-to-end encryption, RSA, ElGamal, SHA-256, digital signature.

A 10-BIT S-BOX GENERATED BY FEISTEL CONSTRUCTION FROM CELLULAR AUTOMATA

Thomas Prévost
Université Côte d'Azur, France, I3S, Ph.D. student
Bruno Martin
Université Côte d'Azur, France, I3S,Ph.D., full professor

Abstract. In this paper, we propose a new 10-bit S-box generated from a Feistel construction. The subpermutations are generated by a 5-cell cellular automaton based on a unique well-chosen local transition rule and bijective affine transformations. In particular, the cellular automaton rule is chosen based on empirical tests of its ability to generate good pseudorandom output on a ring cellular

ЗМІСТ