УДК 004.056.5

ЗАХИСТ ІНФОРМАЦІЇ ТА КРИПТОГРАФІЇ: СУЧАСНІ КРИПТОГРАФІЧНІ АЛГОРИТМИ – ПОРІВНЯЛЬНИЙ АНАЛІЗ СИМЕТРИЧНИХ І АСИМЕТРИЧНИХ МЕТОДІВ

Іван Мулько

INFORMATION SECURITY AND CRYPTOGRAPHY: A COMPARATIVE ANALYSIS OF MODERN CRYPTOGRAPHIC ALGORITHMS – SYMMETRIC VS ASYMMETRIC METHODS

Ivan Mulko

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *A comprehensive analysis of modern cryptographic algorithms has been conducted, comparing symmetric (AES, 3DES) and asymmetric (RSA, ECC) encryption methods. Their advantages, disadvantages, and areas of application have been examined in the context of information security. The relevance of a hybrid approach, combining both methods to enhance data protection efficiency, has been substantiated. The significance of the topic is emphasized in light of the ongoing development of quantum technologies.*

У сучасному цифровому світі питання захисту інформації набуває надзвичайної актуальності. Зростання обсягів електронного документообігу, розвиток електронної комерції, онлайн-банкінгу, хмарних технологій та глобального Інтернету речей створює потребу в надійних засобах збереження конфіденційності, цілісності та доступності інформації. У цьому контексті криптографія відіграє ключову роль, оскільки вона забезпечує фундаментальні механізми захисту даних від несанкціонованого доступу. Основу сучасної криптографії становлять два головні підходи: симетричне та асиметричне шифрування. Їх порівняння дозволяє краще зрозуміти особливості, переваги й недоліки кожного методу та обрати оптимальний варіант для конкретних завдань інформаційної безпеки.

Симетричне шифрування ґрунтується на використанні одного й того ж ключа як для шифрування, так і для розшифрування інформації. Це означає, що обидві сторони комунікації повинні мати доступ до одного й того ж секретного ключа. Одним із найвідоміших сучасних симетричних алгоритмів є AES (Advanced Encryption Standard), який прийнято як міжнародний стандарт і широко використовується в державному, військовому й комерційному середовищі. Симетричні алгоритми, такі як AES, Blowfish або ChaCha20, характеризуються високою швидкістю виконання та ефективністю при обробці великих обсягів даних, що робить їх особливо придатними для масового шифрування файлів, дисків або мережевого трафіку. Проте головним недоліком симетричних методів є проблема розповсюдження ключів: безпечна передача секретного ключа між сторонами до встановлення зв’язку є надзвичайно складним завданням, особливо в умовах відкритих мереж [1-3].

У дослідженні Baig M. H. M. і співавторів [2] проведено ґрунтовний порівняльний аналіз трьох поширених криптографічних алгоритмів – AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman) та 3DES (Triple Data Encryption Standard) – з акцентом на швидкодії та продуктивності при виконанні шифрування й дешифрування даних. Автори вивчали ці алгоритми на основі ряду критеріїв, серед яких головними є швидкість обробки інформації, споживання обчислювальних ресурсів, складність реалізації, рівень безпеки та придатність для реального часу. Згідно з результатами експериментів, AES продемонстрував

найкращі показники швидкодії, що пояснюється його сучасною блоковою структурою, оптимізованою для апаратного та програмного прискорення, а також ефективним механізмом заміни, перестановки та ключового розширення. Алгоритм обробляє дані блоками по 128 біт і підтримує довжину ключа 128, 192 або 256 біт, що забезпечує як високу продуктивність, так і надійний рівень безпеки. Автори відзначають, що AES виконує шифрування та дешифрування значно швидше, ніж 3DES і RSA, особливо при роботі з великими обсягами даних або в умовах обмежених ресурсів, таких як мобільні пристрої чи вбудовані системи.

У свою чергу, 3DES, який є модифікацією застарілого DES, виявився найбільш ресурсоємним і повільним серед досліджених алгоритмів. Його механізм потрійного шифрування – тобто послідовне застосування DES тричі до кожного блоку даних – призводить до значного навантаження на систему та збільшення часу обробки. Незважаючи на те, що 3DES забезпечує вищу безпеку, ніж оригінальний DES, його ефективність уже не відповідає сучасним вимогам, що, як зазначають дослідники, обмежує сферу його використання [2].

RSA належить до асиметричних алгоритмів і має зовсім іншу архітектуру, що базується на складності факторизації великих простих чисел. У дослідженні підкреслюється, що RSA є надто повільним для шифрування великих масивів даних. Його перевага полягає не у швидкодії, а в можливості безпечної передачі ключів і реалізації цифрового підпису. Однак через високі обчислювальні витрати, RSA здебільшого використовується в комбінації з симетричними алгоритмами, де він виконує допоміжну функцію [2].

Автори доходять висновку, що AES є найоптимальнішим варіантом серед розглянутих алгоритмів для використання в реальному часі – наприклад, у потоковому шифруванні, VPN-з'єднаннях, бездротовому зв’язку та хмарних обчисленнях. Його висока швидкість, низьке споживання ресурсів і адаптивність до різних платформ роблять його провідним стандартом сучасної симетричної криптографії [2].

На відміну від симетричного, асиметричне шифрування (також відоме як криптографія з відкритим ключем) використовує пару ключів: відкритий і закритий. Відкритий ключ може бути вільно розповсюджений і використовується для шифрування повідомлень, а закритий ключ зберігається в таємниці і служить для розшифрування. Один із найвідоміших алгоритмів асиметричного шифрування – RSA (Rivest–Shamir–Adleman), а також більш сучасні еліптичні криві (ECC) та алгоритм ElGamal. Перевага такого підходу полягає в усуненні потреби у безпечному каналі для обміну ключами, оскільки відкритий ключ може передаватися відкрито. Крім того, асиметричні алгоритми забезпечують додаткову функціональність, наприклад, створення цифрових підписів, що дозволяє перевірити справжність та цілісність даних, а також автентичність відправника.

Згідно з аналізом Yafei Xie, RSA залишається найпоширенішим алгоритмом у публічній криптографії, хоча ElGamal і ECC пропонують кращу продуктивність при меншій довжині ключа, що особливо важливо в умовах обмежених ресурсів [4]. Це підтверджується також у дослідженні Tuo Zehao, де підкреслюється, що інтегроване використання AES і RSA у гібридних системах дозволяє досягти балансу між продуктивністю й безпекою, поєднуючи переваги обох типів алгоритмів [3].

У контексті розвитку штучного інтелекту та підвищеної обчислювальної потужності новітніх систем, питання ефективності криптографічних алгоритмів набуває нового виміру. У статті Kshetri та ін. акцент зроблено на тому, що зростання ролі AI створює як нові виклики, так і нові можливості для криптографії. Вони аналізують ефективність сучасних симетричних і асиметричних алгоритмів у контексті автоматизованої обробки даних, де симетричні методи переважають у продуктивності, а асиметричні – у масштабованості та інтегрованій безпеці [1].

Проте асиметричне шифрування значно поступається симетричному у швидкості. Через складність математичних операцій (наприклад, операцій з великими простими числами) асиметричні алгоритми споживають більше обчислювальних ресурсів і часу. Саме тому на практиці обидва методи часто комбінуються в так званих гібридних криптографічних системах. У таких системах асиметричне шифрування використовується для безпечного

обміну симетричними ключами, після чого самі дані шифруються швидким симетричним методом. Цей підхід широко застосовується, наприклад, у протоколі TLS, що забезпечує захищене з'єднання в мережі Інтернет.

Окремо варто розглянути й питання стійкості до атак, зокрема квантових. У сучасних умовах загроза квантових обчислень ставить під сумнів довгострокову надійність багатьох асиметричних алгоритмів, включаючи RSA, що ґрунтується на складності факторизації великих чисел. У той же час симетричні алгоритми, як показує аналіз Shaikh та ін., залишаються більш стійкими до квантових атак завдяки іншому механізму роботи – збільшення довжини ключа може істотно ускладнити злам навіть за допомогою квантового комп'ютера [4].

Загалом, симетричні алгоритми характеризуються високою швидкістю, низькими вимогами до ресурсів і ефективністю при роботі з великими обсягами даних, однак мають складність у безпечному розповсюдженні ключів. Асиметричні методи, навпаки, полегшують управління ключами та забезпечують кращу безпеку в розподілених мережах, однак поступаються у швидкодії. Як підсумовують дослідники, найефективнішою моделлю в умовах сучасних викликів є використання гібридних систем, що поєднують обидва типи алгоритмів: симетричні – для шифрування великих масивів даних, а асиметричні – для безпечної передачі ключів і автентифікації [1; 3].

Порівнюючи ці два методи, можна дійти висновку, що вибір між симетричним та асиметричним шифруванням залежить від конкретного контексту використання. Якщо мова йде про шифрування великих масивів даних на одному пристрої або в закритій системі, симетричне шифрування буде оптимальним рішенням. Якщо ж важливо забезпечити захищений обмін інформацією між віддаленими сторонами без попереднього обміну секретами – варто звернутися до асиметричного шифрування.

У світлі загроз квантових обчислень, які потенційно здатні зламати більшість класичних асиметричних алгоритмів, тривають активні дослідження в галузі постквантової криптографії. Уже сьогодні розробляються нові алгоритми, стійкі до атак квантових комп'ютерів, і в майбутньому вони, ймовірно, замінять сучасні криптографічні стандарти.

Отже, симетричне і асиметричне шифрування – це два взаємодоповнювальні підходи до захисту інформації, кожен з яких має свої переваги, недоліки та сферу застосування. Їх ефективна комбінація є ключем до побудови надійних систем кібербезпеки в умовах постійно зростаючих інформаційних ризиків і технологічних викликів.

Бібліографія

1. Naresh Kshetri, Mir Mehedi Rahman, Md Masud Rana, Omar Faruq Osama, James Hutson AlgoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography – A comparative analysis in AI era. *arXiv*. 2024. URL: https://arxiv.org/abs/2412.15237 (дата звернення: 13.05.2025).
2. Baig M. H. M., Ul Haq H. B., Habib W. A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance. *Management Science Advances.* 2024. № 1(1). P. 20-30. DOI: https://doi.org/10.31181/msa1120244 (дата звернення: 13.05.2025).
3. Zehao Tuo A Comparative Analysis of AES and RSA Algorithms and Their Integrated Application. *Theoretical and Natural Science*. 2023. T. 25. P. 28–35. DOI: https://doi.org/10.54254/2753-8818/25/20240893 (дата звернення: 13.05.2025).
4. Yafei Xie A Comparative Analysis of Public Key Cryptographic Algorithms: RSA, ElGamal, and Elliptic Curve Encryption. Theoretical and Natural Science. 2023. T. 14. P. 91–95. DOI: https://doi.org/10.54254/2753-8818/14/20240886 (дата звернення: 13.05.2025).