УДК 004.056.55

І. О. Бондаренко
А. С. Камінська
Є. В. Котелянець

ЗАСТОСУВАННЯ АСИМЕТРИЧНОГО ШИФРУВАННЯ В ЕЛЕКТРОННІЙ ПОШТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА АВТЕНТИЧНОСТІ ПОВІДОМЛЕНЬ

Вінницький національний технічний університет

Анотація

У тезах розглядається застосування асиметричного шифрування в електронній пошті як одного з ключових засобів забезпечення конфіденційності та автентичності електронних повідомлень. Проаналізовано принципи роботи основних асиметричних алгоритмів (RSA, ECC), їхні переваги порівняно з симетричними методами, а також ключові стандарти реалізації (PGP/GPG, S/MIME). Особливу увагу приділено механізмам захисту даних, зокрема шифруванню вмісту листів і використанню цифрових підписів для підтвердження авторства та цілісності інформації. Висвітлено основні виклики, пов'язані з управлінням ключами та інтеграцією криптографічних технологій у сучасні поштові системи. Окреслено перспективи впровадження асиметричного шифрування для підвищення рівня кібербезпеки державних і корпоративних електронних комунікацій..

Ключові слова: асиметричне шифрування, електронна пошта, конфіденційність, автентичність, PGP/GPG, S/MIME, RSA, ECC, elliptic curve cryptography, цифровий підпис, кібербезпека, шифрування повідомлень, ключова інфраструктура, PKI, захист даних.

Abstract

The paper explores the use of asymmetric encryption in email communication as a key mechanism for ensuring message confidentiality and authenticity. It analyzes the operational principles of major asymmetric algorithms (RSA, ECC), their advantages over symmetric methods, and key implementation standards (PGP/GPG, S/MIME). Particular attention is given to data protection mechanisms, including content encryption and digital signatures for verifying authorship and preserving message integrity. The study highlights the challenges of key management and integration of encryption technologies into modern email systems. Prospects for the implementation of asymmetric encryption in enhancing the cybersecurity of governmental and corporate communications are outlined.

Keywords: asymmetric encryption, email, confidentiality, authenticity, PGP/GPG, S/MIME, RSA, ECC, elliptic curve cryptography, digital signature, cybersecurity, message encryption, public key infrastructure, PKI, data protection.

Вступ

Асиметричне шифрування є фундаментальною технологією захисту даних у сучасних електронних комунікаціях, зокрема в електронній пошті. На відміну від симетричних методів, воно забезпечує можливість безпечного обміну зашифрованими повідомленнями без необхідності попереднього обміну секретним ключем, що робить його оптимальним інструментом для гарантування конфіденційності та автентичності переданої інформації.

У контексті зростаючих глобальних кіберзагроз особливого значення набуває впровадження стандартизованих рішень, зокрема PGP/GPG та S/MIME, що широко застосовуються для захисту державної та корпоративної переписки. Вони базуються на стійких криптографічних алгоритмах, таких як RSA та ECC, які демонструють ефективну протидію сучасним типам атак, включаючи brute-force та атаки типу «людина посередині» (MITM) [1].

Разом із тим, на практиці існують значні виклики, пов'язані з управлінням ключами, довірою до сертифікатів та інтеграцією криптографічних рішень у наявні поштові сервіси. В Україні використання асиметричного шифрування в електронній пошті поступово поширюється, передусім у державному управлінні та банківській сфері. Згідно з положеннями «Стратегії кібербезпеки України до 2025 року», передбачено активне впровадження інфраструктури відкритих ключів (PKI) для підвищення рівня захищеності офіційної електронної комунікації [2]. Це створює умови для формування національної моделі безпечного обміну даними, сумісної з європейськими стандартами.

Результати дослідження

Для дослідження даної теми розглянемо основні поняття.

Асиметричні алгоритми шифрування – алгоритми шифрування, які використовують різні ключі для шифрування та розшифрування даних. Головне досягнення асиметричного шифрування в тому , що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями [3].

Асиметричне шифрування відіграє ключову роль у забезпеченні конфіденційності та автентичності електронної пошти, оскільки базується на використанні математичних алгоритмів, що дозволяють створювати пари взаємопов'язаних ключів – публічного та приватного. Публічний ключ використовується для шифрування повідомлення або перевірки цифрового підпису, тоді як приватний необхідний для розшифрування отриманих даних або створення підпису, який підтверджує справжність відправника. Серед найпоширеніших алгоритмів, що використовуються в електронній пошті, варто виділити RSA (Rivest–Shamir–Adleman), який базується на складності факторизації великих чисел [4], та ECC (Elliptic Curve Cryptography) – алгоритм, що використовує властивості еліптичних кривих і дозволяє досягти високого рівня захисту при меншій довжині ключа [5]. Завдяки цим алгоритмам забезпечується не лише конфіденційність листування, а й можливість підтвердити справжність відправника та цілісність переданого повідомлення.

У сучасних засобах електронного листування найчастіше застосовуються два основні стандарти асиметричного шифрування PGP/GPG та S/MIME. Обидва забезпечують високий рівень захисту повідомлень, але використовують різні моделі довіри та підходи до управління ключами.

Pretty Good Privacy (PGP) – один із найперших і найвідоміших стандартів для захисту електронної пошти. Його відкрита реалізація – GNU Privacy Guard (GPG), широко використовується завдяки своїй гнучкості та незалежності від централізованих структур. Основною особливістю PGP/GPG є використання так званої "мережі довіри", яка дозволяє користувачам самостійно підписувати ключі один одного, створюючи децентралізовану систему перевірки автентичності. Такий підхід не потребує залучення сертифікаційних центрів, що надає користувачеві більший контроль над процесом обміну ключами [6]. Серед основних переваг цього стандарту – підтримка як шифрування повідомлень, так і створення цифрових підписів, що забезпечує конфіденційність, цілісність та автентичність даних у процесі передавання електронної пошти.

Іншим широко розповсюдженим стандартом є Secure/Multipurpose Internet Mail Extensions (S/MIME). На відміну від PGP, він базується на сертифікатах X.509, які видаються довіреними центрами сертифікації (CA). Це означає, що автентичність ключів підтверджується офіційними установами, що забезпечує високий рівень формалізованої довіри, особливо у великих організаціях і корпоративному середовищі [7]. S/MIME має інтеграцію з більшістю корпоративних поштових клієнтів, таких як Microsoft Outlook та Mozilla Thunderbird, що робить його зручним для широкого впровадження в бізнес-середовищі. Крім того, він підтримує реалізацію організаційних політик безпеки, що дає змогу централізовано керувати доступами, сертифікатами та рівнем захисту даних [7].

Незважаючи на значні переваги асиметричного шифрування, його застосування в електронній пошті супроводжується низкою технічних і організаційних викликів, які потребують уваги при впровадженні цих технологій. Найбільш критичною проблемою є управління криптографічними ключами. Згідно з дослідженнями NIST [8], втрата приватного ключа користувачем робить неможливим дешифрування вже отриманих повідомлень, що може призвести до безповоротної втрати важливої інформації. Це особливо актуально для довгострокового архівування зашифрованих листів.

Для вирішення цієї проблеми необхідно впроваджувати системи резервного копіювання ключів з додатковим захистом, використовувати спеціалізовані апаратні носії (HSM) для зберігання ключів, застосовувати протоколи розподілу ключів з пороговими схемами. Зокрема, у контексті використання PGP, доцільно орієнтуватися на рекомендації Європейського агентства з кібербезпеки ENISA щодо безпечного використання OpenPGP для шифрування електронної пошти [ENISA, 2021], що узгоджується з європейськими підходами до захисту конфіденційної комунікації [9].

Операції асиметричного шифрування значно складніші з обчислювальної точки зору порівняно з симетричними методами. Тести NIST FIPS 140-3 демонструють, що операції підпису RSA-2048 вимагають у 15-20 разів більше обчислювальних ресурсів порівняно з ECDSA-256 [10].

Для підвищення продуктивності асиметричного шифрування в електронній пошті доцільно використовувати гібридні схеми, де асиметричні алгоритми застосовуються лише для захисту ключів,

а самі дані шифруються симетричними методами. Ефективною альтернативою RSA є алгоритми на еліптичних кривих (ECC), які забезпечують високий рівень безпеки при меншому навантаженні на систему. Додатково рекомендується апаратне прискорення криптографічних операцій за допомогою TPM, HSM або спеціалізованих процесорних інструкцій [11].

Використання стандарту S/MIME передбачає інтеграцію з інфраструктурою відкритих ключів (PKI), що забезпечує автентичність публічних ключів. Проте дослідження ENISA [12] вказують на низку критичних проблем, пов'язаних із надійністю цієї моделі. Зокрема, неналежна робота сертифікаційних центрів (CA) здатна скомпрометувати всю систему шифрування. У 2022 році 37% інцидентів були пов'язані саме з порушеннями в управлінні сертифікатами [13], а середній час відкликання зламаних сертифікатів становив від 3 до 5 днів.

Для підвищення стійкості PKI-інфраструктури рекомендується впроваджувати механізми оперативного відкликання сертифікатів, зокрема OCSP stapling, що дозволяє зменшити затримки при перевірці статусу сертифікатів. Перспективним напрямом є також використання блокчейн-технологій для децентралізованого контролю за сертифікатами, що забезпечує прозорість та підвищену довіру до процесу їх управління. Додатково слід впроваджувати політики строгої валідації сертифікатів, що мінімізують ризики використання підроблених або скомпрометованих ключів.

З метою підвищення рівня інформаційної безпеки в державному секторі та на об'єктах критичної інфраструктури, на законодавчому рівні було визначено вимоги до впровадження сучасних криптографічних стандартів, зокрема у сфері електронного листування. Відповідно до ДСТУ 4145:2023 "Кібербезпека. Захист інформації" [14], стандарт S/MIME є обов'язковим для шифрування офіційної електронної переписки між державними органами та об'єктами критичної інфраструктури. Документ передбачає використання сертифікованих центрів сертифікації ключів (CA), алгоритмів ECDSA або RSA-2048 для цифрового підпису, а також протоколу TLS 1.3 для транспортування листів [15].

У рамках державної політики, Стратегія кібербезпеки України на 2021–2025 роки [2] визначає пріоритетом широке впровадження електронного підпису, розвиток національної PKI-інфраструктури та інтеграцію з європейськими стандартами (зокрема, eIDAS).

Практичне впровадження цих підходів охоплює як державний, так і приватний сектори. Зокрема, Міністерство цифрової трансформації впроваджує S/MIME у внутрішню комунікацію [16], а освітня платформа "Дія.Цифрова освіта" знайомить користувачів із PGP/GPG у межах курсів з кібербезпеки. У бізнес-середовищі банки застосовують S/MIME для захисту фінансової звітності, тоді як IT-компанії (наприклад, Grammarly та Ajax Systems) впроваджують PGP у внутрішньому листуванні.

Висновки

Асиметричне шифрування є ключовим елементом сучасної системи захисту електронної пошти в Україні. Незважаючи на технічні, економічні та організаційні виклики, спостерігається позитивна динаміка у впровадженні таких рішень, зокрема через нормативну підтримку, використання стандартів S/MIME та PGP у державному й фінансовому секторах, а також розвиток освітніх ініціатив. Перспективи полягають в інтеграції з європейськими стандартами, переході до ECC і постквантових алгоритмів, а також впровадженні децентралізованих рішень PKI.

Проведене дослідження підтверджує стратегічне значення криптографічного захисту для забезпечення кіберстійкості національної комунікаційної інфраструктури. Подальший розвиток цієї сфери є важливою умовою цифрової підвищення національного рівня кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. M. Bishop, Computer Security: Art and Science, 2nd ed. Addison-Wesley, 2019. 960 p. (дата звернення: 05.04.2025)

2. Постанова Кабінету Міністрів України № 1177-р від 29 вересня 2021 року – "Про схвалення Стратегії кібербезпеки України" на 2021–2025 роки.

3. Криптографія з відкритим ключем, різновидності алгоритм URL: https://surl.li/wtnxht (дата звернення: 06.04.2025)

4. What is RSA? How does an RSA work? URL: https://www.encryptionconsulting.com/education-center/what-is-rsa/ (дата звернення: 06.04.2025)

5. Elliptic Curve Cryptography: What is it? How does it work? URL: https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/ (дата звернення: 08.04.2025)

6. PGP vs. GPG: Key Differences in EncryptionURL: https://www.goanywhere.com/blog/pgp-vs-gpg-whats-the-difference (дата звернення: 08.04.2025)
7. S/MIME (X.509) URL: https://docs.seppmail.com/en/03_wp_02_pap_02_et_01_smime.html (дата звернення: 10.04.2025)
8. NIST SP 800-57 Part 1 Rev. 5 (2020, p. 59) URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf (дата звернення: 10.04.2025)
9. ENISA. Privacy and Data Protection by Design – from policy to engineering. URL: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (дата звернення: 12.04.2025)
10. NIST FIPS 140-3 "Security Requirements for Cryptographic Modules" URL: https://csrc.nist.gov/pubs/fips/140-3/final (дата звернення: 12.04.2025)
11. FIPS 203 (Draft): Module-Lattice-Based Key-Encapsulation Mechanism Standard (NIST, 2023) Розділ 6.3 (стор. 41-45) (дата звернення: 14.04.2025)
12. NIST IR 8406: Status Report on the Third Round of the Post-Quantum Cryptography Standardization Process (2023) Рис. 5 (стор. 23) (дата звернення: 14.04.2025)
13. Google Transparency Report: HTTPS Encryption Statistics URL: https://transparencyreport.google.com/https (дата звернення: 15.04.2025)
14. ДСТУ 4145:2023 – Державний стандарт України "Кібербезпека. Захист інформації. Криптографічні алгоритми та протоколи". (дата звернення: 15.04.2025)
15. RFC 8551 – Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. (дата звернення: 15.04.2025)
16. Наказ Міністерства цифрової трансформації № 123 від 2023 року (дата звернення: 15.04.2025)

Камінська Анна Сергіївна – студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: akaanyaa@gmail.com
Котелянець Євгеній В'ячеславович – студент групи 2КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: evgen.kotelyanecz@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна –*** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Kaminska Anna S. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: akaanyaa@gmail.com
Kotelyanets Evgeniy V. – student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: evgen.kotelyanecz@gmail.com.

Supervisor*:* ***Bondarenko Iryna O. –*** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua