МАТЕМАТИЧНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ КРИПТОСИСТЕМ З ВІДКРИТИМ КЛЮЧЕМ

Кононенко Ігор Олегович
студент групи МАМм-1-23-1.4.д
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к..ф-м.н., доц.. Жданова Ю.Д.

В епоху цифрової трансформації захист інформації є одним з найважливіших аспектів. Застосування криптосистем з відкритим ключем стало однією з фундаментальних основ сучасної інформаційної безпеки, що забезпечує захищений обмін даними у мережі [1].

Метою дослідження було поставлено глибоке дослідження математичних основ, на яких побудовані сучасні криптосистеми з відкритим ключем, аналіз їх сильних і слабких сторін. Виходячи з мети, основними завданнями стали:

- Огляд існуючих криптосистем з відкритим ключем, зокрема алгоритмів RSA, ElGamal та криптосистем на основі еліптичних кривих [2].
- Вивчення математичних апаратів, що лежать в основі криптографії з відкритим ключем.
- Розроблення математичні моделі для опису роботи криптосистеми з відкритим ключем.

Особливу увагу приділено порівнянню симетричних і асиметричних алгоритмів, що дає змогу зрозуміти унікальність криптосистем з відкритим ключем, де ключ для зашифрування є загальнодоступним, а ключ для розшифрування – закритим. Основними алгоритмами, що використовуються в таких криптосистемах, є RSA (алгоритм Рівеста-Шаміра-Адлемана), ElGamal, DSA (цифровий підпис) та ECC (криптографія на еліптичних кривих). Кожен з них має свої переваги і недоліки, пов'язані з ефективністю та безпекою. Наприклад, RSA заснована на задачі факторизації великих чисел, а ECC використовує властивості еліптичних кривих, що дозволяє знизити обчислювальні ресурси при збереженні рівня безпеки.

Для криптосистем з відкритим ключем важливими задачами є факторизація великих чисел (для RSA) та обчислення дискретного логарифма (для ECC). Стійкість цих криптосистем забезпечується складністю відповідних задач: їх розв'язок потребує значних обчислювальних ресурсів, що унеможливлює злам ключів традиційними методами.

Також досліджуються сучасні методи криптоаналізу, зокрема, алгоритм Шора, здатний розв’язувати завдання факторизації та дискретного логарифмування на квантових комп’ютерах, і алгоритм Полларда, який застосовується для знаходження дискретного логарифма. Наведено приклади оцінки стійкості криптосистем з відкритим ключем, які показують, що з розвитком квантових обчислень виникає необхідність удосконалення існуючих систем захисту [3].

Велику роль в побудові та опису роботи криптосистем з відкритим ключем відіграють математичні моделі, які дозволяють формально аналізувати властивості алгоритмів і проводити теоретичні дослідження.

Зокрема, розглянуто модель криптосистеми RSA та досліджено її ефективність при використанні різних довжин ключів. Також моделюється криптосистема на еліптичних кривих (ECC), яка демонструє високу ефективність при меншій розрядності ключів, порівняно з RSA. Наведено результати експериментів, які порівнюють швидкість шифрування, розшифрування та рівень безпеки, залежно від параметрів криптосистем.

Оцінка показала, що ECC має значні переваги над RSA в умовах обмежених ресурсів, що дозволяє широко використовувати її в мобільних і вбудованих системах. Однак для галузей з високими вимогами до безпеки криптосистема RSA все ще залишається популярною, оскільки забезпечує стабільність і можливість використання дуже великих ключів.

Дослідження показало, що криптосистеми з відкритим ключем є ефективними для захисту інформації, проте їхня стійкість залежить від складності відповідних математичних

задач. Аналіз також показує, що розвиток квантових обчислень ставить під загрозу безпеку класичних криптографічних алгоритмів, зокрема RSA. У зв'язку з цим перспективним є впровадження алгоритмів на еліптичних кривих та дослідження нових постквантових методів шифрування [4,5].

Дослідження методів моделювання криптосистем з відкритим ключем є актуальним і перспективним напрямом для подальшого розвитку захищених комунікацій, зокрема в умовах наближення ери квантових обчислень.

ДЖЕРЕЛА

1. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km

2. Yafei Xie. A comparative analysis of public key cryptographic algorithms: RSA, ELGamal, and elliptic curve encryption. *Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics*, 2023.

3. Jiang, Y., et al. "Lightweight Public Key Encryption in the Post-Quantum Era." *IEEE Xplore*, 2023.

4. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. Cybersecurity: Education, Science, Technique, 1(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158

5. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252