УДК 004.056.5

Чернюк С. І.
Стахов О. Я.

МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ШИФРУВАННЯ В СУЧАСНИХ ІТ-СИСТЕМАХ

Вінницький національний технічний університет

Анотація. *У цих тезах розглянуто можливості та обмеження сучасних криптографічних методів шифрування в інформаційних технологіях. Проведено порівняльний аналіз симетричних та асиметричних алгоритмів шифрування, а також розглянуто перспективи використання гомоморфного шифрування. Окреслено основні виклики, пов'язані з продуктивністю, управлінням ключами та появою квантових обчислень. Зазначено необхідність адаптації існуючих криптографічних підходів до нових загроз та технологій.*

Ключеві слова: шифрування, криптографія, симетричні алгоритми, асиметричні алгоритми, гомоморфне шифрування, постквантова криптографія, інформаційна безпека, кіберзагрози.

Abstract. *These theses observe the possibilities and limitations of modern cryptographic encryption methods in information technology. A comparative analysis of symmetric and asymmetric encryption algorithms is carried out, as well as the prospects for the use of homomorphic encryption. The main challenges associated with performance, key management and the emergence of quantum computing are outlined. The need to adapt existing cryptographic approaches to new threats and technologies is noted.*

Keywords: encryption, cryptography, symmetric algorithms, asymmetric algorithms, homomorphic encryption, post-quantum cryptography, information security, cyber threats.

Вступ

У світі, де обсяг цифрової інформації зростає експоненційно, питання безпеки стають дедалі актуальнішими. Шифрування — один із головних інструментів захисту даних в інформаційних системах. Воно дозволяє забезпечити конфіденційність, цілісність та автентичність інформації під час її зберігання або передавання. У сучасних ІТ-системах використовуються різноманітні криптографічні методи, як симетричні, так і асиметричні, кожен з яких має свої переваги та недоліки залежно від контексту використання.

Актуальність теми зумовлена зростанням кількості кібератак, появою нових алгоритмів шифрування, а також викликами, пов'язаними з постквантовою криптографією та необхідністю забезпечення безпеки в умовах динамічного розвитку технологій. Метою дослідження є аналіз можливостей та обмежень сучасних криптографічних методів шифрування у сфері захисту даних.

Результати дослідження

Криптографічні методи шифрування поділяються на дві основні категорії: симетричні (AES, DES, ChaCha20) та асиметричні (RSA, ElGamal, ECC) [1].

Симетричне шифрування є надзвичайно ефективним з точки зору швидкості та використання ресурсів. Алгоритм AES є де-факто стандартом у багатьох галузях, включаючи банківську сферу, охорону здоров'я, хмарні сервіси [2]. Однак основною проблемою таких систем є передача секретного ключа — якщо він буде перехоплений, уся система стає вразливою.

Асиметричне шифрування, навпаки, базується на парі ключів: відкритому та закритому. Воно зручно використовується для автентифікації, цифрових підписів та безпечного обміну ключами. Найбільш поширеним є RSA, однак він потребує значних обчислювальних ресурсів, особливо при великих об'ємах даних. Еліптична криптографія (ECC) дозволяє досягти високого рівня безпеки з меншими розмірами ключів, що є значною перевагою для мобільних пристроїв [3].

Особливе місце займає гомоморфне шифрування — інноваційний підхід, який дозволяє здійснювати обчислення над зашифрованими даними без їхнього розшифрування. Це відкриває нові горизонти для безпечної обробки чутливої інформації, наприклад, у фінансовій сфері або при обробці медичних даних. Проте сьогоднішні реалізації гомоморфного шифрування є малоефективними з погляду продуктивності, що обмежує їхнє практичне використання [4].

Обмеження криптографічних методів включають:

1. Криптостійкість до квантових атак. Сучасні алгоритми RSA та ECC можуть бути скомпрометовані з появою потужних квантових комп'ютерів [5].
2. Витрати ресурсів. Обчислювальна складність асиметричних алгоритмів обмежує їхнє використання в реальному часі.
3. Управління ключами. Забезпечення безпечного зберігання, генерації та передачі ключів залишається складним завданням.
4. Правове регулювання. Обмеження на використання сильного шифрування в деяких країнах створюють бар'єри для глобальної безпеки [6].

Висновки

Криптографічні методи шифрування є фундаментальним елементом сучасної IT-безпеки. Вони забезпечують захист даних у різних середовищах, від локальних мереж до хмарних інфраструктур. Попри значні досягнення у сфері криптографії, існують певні обмеження, пов'язані з продуктивністю, управлінням ключами та загрозами квантових технологій.

Подальший розвиток цієї галузі потребує вдосконалення існуючих алгоритмів, адаптації до нових викликів та розробки постквантових рішень. Інтеграція криптографії з іншими механізмами безпеки (наприклад, блокчейн, багаторівневе шифрування) дозволить підвищити рівень довіри до цифрових технологій та зменшити ризики кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Євсеєв С.П., Йохов О.Ю., Король О.Г. Гешування даних в інформаційних системах // Монографія Харків: Вид. ХНЕУ. − 2013. – 312 с.
2. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Pearson, 2017. – 752 p.
3. Hankerson D., Vanstone S., Menezes A. Guide to Elliptic Curve Cryptography. – Springer, 2004. – 312 p.
4. Gentry C. Fully Homomorphic Encryption Using Ideal Lattices // STOC'09. – 2009. – Pp. 169–178.
5. Bernstein D.J., Lange T. Post-Quantum Cryptography // Nature, 2017. – Vol. 549. – Pp. 188–194.
6. Diffie W., Landau S. The Export of Cryptography in the 20th Century and the 21st // The World Today. – 2008. – Vol. 64. – Pp. 20–23.

Стахов Олексій Ярославович – доктор філософії, старший викладач кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, Україна.

Чернюк Сергій Іванович – студент групи 2ПІ-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, email: sergblackman1@gmail.com

Stakhov Oleksii Yaroslavovych – PhD, senior teacher of the software department, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Cherniuk Serhii Ivanovych – student of 2ПІ-21б group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, email: sergblackman1@gmail.com