УДК :004.42:620.9 ….

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ АЛГОРИТМІВ ШИФРУВАННЯ В ЗАДАЧІ СТВОРЕННЯ ТА ПЕРЕВІРКИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ З УРАХУВАННЯМ ЕНЕРГОЕФЕКТИВНОСТІ ОБЧИСЛЕНЬ

Мойся І.Ю. – МгІТ2-24, магістрант, *igorega@ukr.net*
Гольдберг М.І. – к.т.н., доцент., *marjanagoldberg@gmail.com*
Київський національний університет технологій та дизайну

Мета роботи - оцінка ефективності різних алгоритмів ЕЦП з точки зору енергоспоживання, часу обробки та безпекового рівня для подальшого використання в енергоощадних ІТ-інфраструктурах.

З розвитком цифрової економіки та переходом до електронного документообігу роль електронного цифрового підпису (ЕЦП) суттєво зросла. ЕЦП забезпечує автентичність, цілісність та невідмовність даних, що є ключовими чинниками інформаційної безпеки.

Проте зі збільшенням обсягу переданих даних та поширенням мобільних і IoT-пристроїв постає новий виклик – забезпечення енергоефективності криптографічних процесів.

Сучасні алгоритми шифрування різняться не лише рівнем стійкості, а й енергоспоживанням при виконанні операцій підпису та перевірки. Це має велике значення для систем, що працюють у реальному часі, наприклад у хмарних платформах, банківських терміналах, інтелектуальних лічильниках, SCADA-системах тощо.

У роботі розглянуто три найбільш поширені алгоритми, що застосовуються у практиці створення ЕЦП:

RSA (Rivest–Shamir–Adleman) – класичний алгоритм на основі факторизації великих чисел.

DSA (Digital Signature Algorithm) – стандартний підхід на базі дискретного логарифмування.

ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм на основі еліптичних кривих, що вважається більш енергоефективним.

Для кожного алгоритму оцінювались: часу генерації ключів, створення та перевірки підпису; використання оперативної пам’яті; середнього енергоспоживання процесора під час виконання операцій; розміру підпису у байтах (як фактору передачі даних через мережу).

Отримані результати показали, що застосування ECDSA забезпечує баланс між рівнем криптографічної стійкості та енергоспоживанням, що робить його доцільним вибором для енергоефективних систем, зокрема у мобільних пристроях, розподілених сенсорних мережах і «розумних» енергетичних системах (smart grid).

Результати свідчать про те, що енергоспоживання криптографічних алгоритмів має суттєве значення у загальній енергоефективності IT-інфраструктури.

Вибір алгоритму шифрування впливає не лише на швидкодію, а й на теплове навантаження процесора, стабільність роботи серверів і тривалість автономної роботи пристроїв.

В умовах зростання масштабів цифровізації енергетичного сектору (наприклад, впровадження систем обліку, моніторингу, автоматизованих контролерів) доцільно орієнтуватися на алгоритми, які поєднують безпеку й енергоощадність.

Перспективним напрямом подальших досліджень є використання гібридних методів – поєднання симетричного й асиметричного шифрування з динамічним перемиканням залежно від обчислювального навантаження та поточного енергетичного стану системи.

Висновки

- Проведено порівняльний аналіз алгоритмів RSA, DSA та ECDSA з позиції енергоефективності при створенні й перевірці електронного цифрового підпису.
- Встановлено, що алгоритми на основі еліптичних кривих (ECDSA) забезпечують найкраще співвідношення між рівнем безпеки, швидкодією та енергоспоживанням.
- Використання енергоефективних криптографічних методів сприяє зниженню навантаження на сервери, економії енергії IT-інфраструктури та підвищенню стійкості систем захисту інформації в енергетичній галузі.
- Розроблені підходи можуть бути інтегровані у системи електронного документообігу, банківські API, а також у смарт-енергетичні рішення, де безпека та енергоефективність є критично важливими.

Список використаних джерел:

1. Stallings W. *Cryptography and Network Security: Principles and Practice.* – 8th ed. – Pearson, 2023.

2. Koblitz N., Menezes A. *Elliptic Curve Cryptography: The Serpent's Smile.* – Contemporary Mathematics, Vol. 637, 2015.

3. Gupta S., Kalra S. *Energy-Efficient Cryptographic Techniques for IoT Devices.* – *IEEE Internet of Things Journal*, 2021. – DOI: 10.1109/JIOT.2021.3087549.

4. RFC 4492 – *Elliptic Curve Cryptography (ECC) Cipher Suites for TLS.* – https://www.rfc-editor.org/rfc/rfc4492.

5. Артеменко О. М., Костюк В. В. *Сучасні методи криптографічного захисту інформації.* – Київ : КНУ ім. Т. Шевченка, 2020. – 178 с.

6. ДСТУ ISO/IEC 14888-3:2017. *Інформаційні технології. Методи криптографічного захисту. Цифрові підписи.* – Київ : УкрНДНЦ, 2017.