learning-based network anomaly detection. Cluster Computing. 2019. Vol. 22. P. 949–961. DOI: 10.1007/s10586-017-1117-8.
4. Chalapathy R., Chawla S. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407. 2019. 50 p.
5. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 800 p.
6. Hinton G. E., Salakhutdinov R. R. Reducing the dimensionality of data with neural networks. Science. 2006. Vol. 313, № 5786. P. 504–507.
7. Іванченко Є. І., Рижаков М. М. Узагальнена модель прогнозування та виявлення кібербезпекових аномалій на основі штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/823.
8. Рижаков М. М. Моделі та методи виявлення кіберінцидентів у телекомунікаційних мережах критичної інфраструктури : дис. … д-ра філософії : 125 / Держ. ун-т інформ.-комунікац. технологій. Київ, 2025. URL: https://duikt.edu.ua/uploads/p_2958_82196938.pdf.
9. Pang G., Shen C., Cao L., Hengel A. v. d. Deep learning for anomaly detection: A review. ACM Computing Surveys. 2021. Vol. 54, № 2. P. 1–38. DOI: 10.1145/3439950.

## Програмний засіб для шифрування у системі залишкових класів

УДК 004.424

Олег Момотюк[1], Михайло Голембйовський[2], Михайло Касянчук[3]

*Західноукраїнський національний університет,*
*[1]momotjuk98@gmail.com, [2]mykhailo.2097@gmail.com, [3]kasyanchuk@ukr.net*

У сучасних інформаційних системах зростає потреба у криптографічних алгоритмах, які поєднують достатній рівень захисту даних із високою швидкодією та можливістю ефективної реалізації в умовах обмежених обчислювальних ресурсів [1]. Одним із перспективних підходів до підвищення продуктивності криптографічних операцій є використання системи залишкових класів (СЗК) [2, 3]. Її перевага полягає в тому, що велике число може бути подане як набір залишків за декількома попарно взаємно простими модулями. У такому представленні арифметичні операції виконуються незалежно для кожного модуля, що створює природні передумови для паралельної обробки даних. Це дає змогу зменшити складність обчислень над великими числами та підвищити швидкодію алгоритмів, які використовують модульну арифметику.

Дана робота присвячена розробці програмного засобу для шифрування в СЗК. Запропонований підхід змінює логіку обробки повідомлення: криптографічне перетворення застосовується не до окремих символів, а до числового блоку відкритого тексту. Такий блок розкладається на залишки за системою модулів, після чого для кожного залишку виконується окреме криптографічне перетворення. Отримані змінені залишки об’єднуються у зашифроване число за допомогою китайської теореми про залишки (КТЗ).

Математична модель алгоритму передбачає кілька послідовних етапів. Спочатку відкритий текст кодується у числове представлення. Далі перевіряється коректність параметрів: модулі мають бути попарно взаємно простими, значення множників повинні мати обернені елементи за відповідними модулями, а числовий блок повідомлення має бути меншим за добуток усіх модулів. Після цього для кожного модуля обчислюється залишок, виконується криптографічне перетворення, а результат збирається у компактний шифртекст. Розшифрування відбувається у зворотному порядку: із зашифрованого числа відновлюються змінені залишки, далі — початкові залишки, після чого КТЗ дозволяє отримати вихідний числовий блок і декодувати його у текст.

Програмна реалізація виконана мовою Python із використанням фреймворку FastAPI. Архітектура програмного засобу побудована за принципом розділення відповідальностей і включає рівень маршрутизації, рівень бізнес-логіки та модуль математичних утиліт. Рівень маршрутизації забезпечує обробку HTTP-запитів до ендпоінтів шифрування, розшифрування, генерації параметрів і вимірювання продуктивності. Рівень сервісів реалізує основну логіку шифрування в СЗК, тоді як допоміжний математичний модуль містить функції для обчислень за КТЗ, перевірки взаємної простоти модулів і генерації ключових параметрів. Валідація вхідних даних здійснюється засобами Pydantic, що зменшує ризик некоректного використання алгоритму.

Для оцінювання продуктивності реалізовано механізм вимірювання часу виконання криптографічного ядра за допомогою високоточного таймера. При цьому з вимірювань виключаються допоміжні операції. Тестові приклади демонструють, що операції шифрування та розшифрування виконуються за частки мілісекунди, що підтверджує практичну придатність запропонованого підходу для швидкої обробки коротких текстових повідомлень. Приклад шифрування наведено на рис. 1.

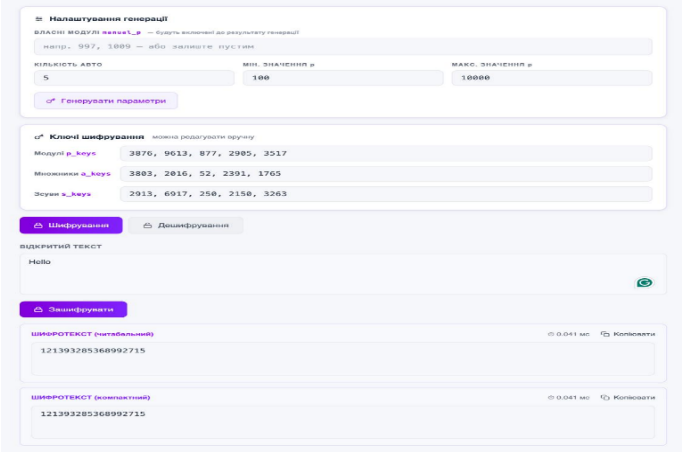


Рис.1. Приклад шифрування

Отже, розроблений програмний засіб демонструє можливість практичного використання СЗК для модифікації класичних криптографічних алгоритмів. Поєднання криптографічного перетворення з багатомодульним представленням даних дозволяє ускладнити структуру шифротексту, розподілити інформацію між кількома модулями та створити основу для паралельної обробки. Подальші дослідження доцільно спрямувати на поглиблений криптоаналіз запропонованого методу, оптимізацію вибору модулів, порівняння з сучасними симетричними алгоритмами та реалізацію обчислень на апаратних платформах, зокрема FPGA або GPU.


1. 1. Nieles M., Dempsey K., Pillitteri V. *An Introduction to Information Security*. Gaithersburg : NIST, 2017. 101 p..
2. 2. Kasianchuk M. M., Yakymenko I. Z., Nykolaychuk Y. M. Symmetric Cryptoalgorithms in the Residue Number System. *Cybernetics and Systems Analysis*. 2021. Vol. 57. P. 329–336. https://doi.org/10.1007/s10559-021-00358-6.
3. 3. Nykolaychuk Ya. M., Yakymenko I. Z., Vozna N. Ya., Kasianchuk M. M. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis*. 2022. Vol. 58, No. 4. P. 611–618. https://doi.org/10.1007/s10559-022-00494-7.


## Проєктування захищеної архітектури для оцінювання ігор LUDARA з використанням технології Node.js та принципів Security-by-Design

УДК 004.42

Мороз Даниїл[1], Мудрик Іван[2]

*Тернопільський національний технічний університет імені Івана Пулюя,*
*[1]danyil_moroz1301@tntu.edu.ua, [2]i1mudryk@tntu.edu.ua*

Теперішній ринок відеоігор демонструє стрімке зростання: за даними аналітичних агентств, кількість активних гравців у світі перевищує 3 мільярди осіб, а обсяг галузі щорічно збільшується на 8–10% [1]. Попри це, існуючі платформи для оцінювання ігор стикаються з низкою проблем інформаційної безпеки: ризиками компрометації персональних даних користувачів, вразливостями відкритих API, а також маніпуляцією рейтингами за допомогою автоматизованих скриптів (ботів). Метою роботи є проєктування та розробка безпечної архітектури веб-платформи «Ludara», що базується на принципах Security-by-Design із використанням технологічного стеку Node.js.

Архітектура платформи реалізована за принципом чіткого розмежування рівнів доступу та відповідальностей. Серверна частина побудована на Node.js з фреймворком Express.js, клієнтська — на React з використанням Vite [2]. Для гарантування цілісності даних обрано реляційну СУБД PostgreSQL. Взаємодія з базою даних здійснюється через ORM-бібліотеку Prisma, що автоматично параметризує запити, унеможливлюючи атаки типу SQL-ін'єкцій, та забезпечує типобезпечність. Автентифікація реалізована за протоколом на основі JWT-